SECURE TECHNOLOGY ALLIANCE

NOVEMBER 2017

SECURE TECH TALK

A quarterly newsletter for members and friends of the Alliance

The ABCs of Healthcare Security

The incidences of cyberattacks and ransomware are on the rise and the steps necessary to secure information networks are top of mind for chief security officers everywhere, but particularly for our nation's healthcare providers. When I was invited to participate in a healthcare security conference recently, the solutions I heard from every security vendor could all be categorized as ABC solutions – Anything But Cards. Read more about the shortcomings of ABC solutions and how smart cards could fix what is wrong with the healthcare IT security. In December, look for the 2017 Secure Technology Alliance Annual Review in this space, providing a year's worth of activities, news and accomplishments of our organization and its members.

Click to Read Letter ...

Feature Article:
Contactless Payment-Enabled Wearables: A Primer

Wearables, as a general category, cover wide variety of device types – from smartwatches to rings to wristbands to clothing – using different communications and security technologies. The total wearables market is expected to have significant growth, and market growth for connected devices that can be used for a variety of functions presents opportunities for device manufacturers, service providers and the payments industry. This quarter's article provides an overview of the benefits of and technologies used in most common wearables implementations today.

Click to Read More …

DIGITAL INNOVATION ALLIANCE
SECURE TECHNOLOGY ALLIANCE LATIN AMERICAN CHAPTER

Latin America Letter:
A Digital Transition

I am very pleased to announce that the Smart Card Alliance Latin America (SCALA) chapter has changed its name to Digital Innovation Alliance (DIA). This move will allow us to expand our mission – and the services we provide to members – to support the evolution towards a digital society. Learn more in my letter about this expansion of the chapter, and the work we plan to do ensure we remain a resource for members and technology professionals.

Click to Read More …

In This Issue:

On the Web:

Upcoming Event:

Joint 2018 Payments Summit / ICMA Expo and U.S. Payments Forum Meeting
March 26-29, 2018
Omni Orlando Resort at ChampionsGate, Championsgate, FL
https://www.stapayments.com/

The ABCs of Healthcare Security

Dear Members and Friends of the Alliance,

At a recent healthcare security conference where I was a speaker, much of the discussion from individual speakers and panel discussions focused on the challenges facing hospital system chief information security officers (CISOs) in managing the risks associated with the escalating frequency and sophistication of cyber-attacks and ransomware within the healthcare industry.

We heard from security experts about a variety of solutions to address the risks, including moving more systems into the cloud to reduce the number of attack surfaces, implementing advanced email security solutions to reduce phishing attacks, restricting vendor access to critical patient information systems, and installing advanced analytics software to detect workplace behavior of employees that would provide alerts to insider threats. We also heard many other recommendations.

I label all these approaches to better healthcare security as ABC solutions – Anything But Cards.

The root causes of every cyber threat are poor identity management and authentication practices. Most attacks are the result of unauthorized access by individuals who gain control of privileged credentials and move laterally and vertically within networks to find access to protected files or command and control systems. That then allows them to steal data or inflict harm on networked services. Yet not a single speaker at the conference (other than myself) proposed that CISOs use multifactor authentication – despite the fact that the common thread amongst these defensive approaches was controlling who has access to sensitive patient information and critical hospital operations systems before a cyber event occurs.

When it was my turn to speak, I used two examples of industries addressing their security problems with chip cards: how the payments industry are using chip cards to for bank card authentication; and how the government is issuing chip cards for identity credentials like e-passports for citizens and federal worker IDs. I also explained how both markets are including a second biometric factor for security. I pointed out that it took major cyber incidents, like the Target and Home Depot data breaches in payments, and the Office of Personnel Management (OPM) data breach within the government, to spur the industries into action to implement smart card-based systems.

What is it going to take to get healthcare to invest in this proven technology? What will be the bellwether incident for the healthcare industry that is going to get CISOs to demand a solution from health IT vendors like McKesson, GE Healthcare, Siemens, and IBM that solves the identity management problem with secure identity cards rather than adding on more, and increasingly less effective, proprietary ABC solutions?

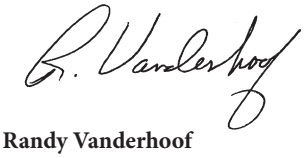
According to the 2017 Verizon Data Breach Investigations Report, the healthcare industry was second only to financial institutions in the frequency of data breaches. Stolen and/or weak passwords were a common issue among the reported breaches, the report explained. Eighty-one percent of hacking-related breaches used either stolen or weak passwords. The Verizon report recommends two-factor authentication to help organizations limit potential damage from lost or stolen credentials.

Healthcare security officers and CEOs are not lacking awareness of the threats they are facing. Nor are they lacking the availability of cost-effective, proven strong authentication solutions. Health IT vendors are capable of implementing multi-factor authentication to replace user names and passwords to access the most critical hospital systems. These IT vendors simply are not being asked to build this level of security into the hardware and software they sell and support. If one or more hospital CEOs gets fired, like the CEO of Target and the Director of the Office of Personnel Management did after their organizations' cyberattacks, then perhaps we will see some progress made. Don't say we didn't warn you!

Next month there will not be a newsletter from the Secure Technology Alliance. We are going to publish the 2017 Annual Review, a full-color, 76-page publication highlighting the programs, events and council activity the Alliance and its members experienced throughout the year.

I wish you all a happy holiday season, and thank you for your support of our organization.

Sincerely,



Randy Vanderhoof
Executive Director, Secure Technology Alliance
rvanderhoof@securetechalliance.org

A Digital Transition

Dear Members and Friends of the Alliance,

I am pleased to announce that Smart Card Alliance Latin America (SCALA) chapter has changed its name to Digital Innovation Alliance (DIA). After more than ten years supporting and promoting the use of smart cards in different sectors, and with the understanding of the needs of the market regarding the evolution of technology, the SCALA Advisory Board recognized that the needs of the market regarding technology evolution have changed. After thoughtful consideration, they agreed that it was important to expand the organization's mission and member services to support the evolution towards a digital society.

Through many years SCALA had led the discussions on the movement from electronic to digital in multiple sectors, such as: methods of payments, identification, biometrics, cybersecurity, and smart communities. Many of these sectors began their path towards digital by introducing smart cards and related components, using chip technology in different form factors to provide both security and a better user experience. Moreover, they have expanded these concepts using virtual or embedded secure elements to ensure that security and functionality expanded into the digital realm. This has created new opportunities for our organization to continue its leadership in providing a forum for cutting edge discussions.

The Digital Innovation Alliance will remain a promotional and educational resource for our members and technology professionals, advocating for the implementation of technological solutions that can improve the community quality of life. We are working on increasing the number of white papers and documents that will provide objective resources regarding these subjects, as well as training programs at our Digital Center of Excellence. To accomplish this mission, DIA's activities will be based on four pillars: convergence, or the integration of different sectors by implementing technology; interoperability, geared to connect information that will facilitate decision-making processes; innovation, the key to generating changes; and collaboration, ensuring that industry leaders find a common ground.

As an organization, the Digital Innovation Alliance believes that by helping with technology, we contribute to the overall improvement of our societies and sectors by making these processes user-, citizen-, and human-centric.

I will also want to take this opportunity to inform all our members and friends that the Digital Innovation Alliance has taken a leadership role in helping to create the framework for developing smart cities in the Americas, working with different sectors in the ecosystem to collaborate and expand concepts that will lead to a roadmap. In this effort, we have been joined by mayors and different presidents of the Smart Cities Business Institute of Americas (ISCBA) to create a community, develop content, and recognize expertise.

Our concept for smart communities is based on establishing the citizen as the center of our society, where all things are meant to connect to improve their quality of life. This means that technologies surrounding identification and unique identifiers become very important building building a better society.

Finally, we would like to thank all of our members for their continuous support and belief in the evolution of our organization. Our achievements are only possible because of their advice and team efforts. We also encourage new companies and professionals to engage with the new Digital Innovation Alliance to help us to improve the digital technology industry within Latin America and the Caribbean, feel free to contact us or visit our new website www.thedigitalalliance.org.

Sincerely,

Edgar Betts
Director, Smart Card Alliance Latin America (SCALA)
ebetts@smartcardalliance.org
www.sca-la.org

Contactless Payment-Enabled Wearables: A Primer

Wearables, as a general category, cover wide variety of device types – from smartwatches to rings to wristbands to clothing – using different communications and security technologies. The total wearables market is expected to have significant growth, with a recent Gartner report estimating that 310.4 million wearable devices will be sold in 2017, growing to over 504 million by 2021. [1]

This market growth for connected devices that can be used for a variety of functions presents opportunities for device manufacturers, service providers and the payments industry. Payment-enabling wearables can make payment easier and more convenient for consumers. BI Intelligence estimates that 62 percent of wearable device shipments will include payments functionality by 2020. [2]

This month's article provides an overview of the benefits of and technologies used in most common wearables implementations today: wearables that support contactless transactions using technology that complies with ISO/IEC 14443 with security based on hardware secure elements.

Benefits of Payment-Enabled Wearables

Using wearable devices for payment is an idea that's been sought after for years. Over 10 years ago, the payment industry introduced payment stickers as a universal alternative payment form factor. Payment now encompasses many complimentary form factors, including stickers and a wide variety of wearables.

The key benefits of payment-enabled wearables for consumers, issuers, merchants, prepaid program managers/event organizers, and OEMs/device manufacturers are summarized below.

Consumers. Wearable devices present a unique advantage for end users when embodying the applications such as credit, debit or prepaid payment, event passes or transit payment. The wearable device is always with the user, therefore less subject to loss. It is ready for use at the time of redemption. Convenience is a primary value proposition for the end user.

Wearable devices simplify a user's daily activity, which is especially beneficial for those activities with repeat use. Payment-enabled wearables best fulfill their purpose when other forms of payment are not available or are less convenient to use. Examples include: paying with a wearable for a refreshment or snack at an event where a purse or wallet isn't otherwise necessary; buying a quick coffee or daily groceries;

paying for transit system access. All of these daily consumer activities are made more convenient with a wearable device like a wristband or a ring.

Issuers. Wearables benefit issuers by enhancing the frequency of use of a payment credential by providing consumers with a new and convenient form of payment. Wearables offer a significant benefit to the issuer since, much like bank-issued cards, wearables can carry branding. A branded wristband used for payment and access can provide significant marketing benefits to an issuer. Compared to cards that consumers keep in their wallets, a branded wearable device that's worn on the wrist remains top-of-mind – not just top-of-wallet – and is visible to others around the consumer wearing the device.

Merchants. Frequency and convenience are key drivers to increase sales and consumer loyalty. Merchants can increase loyalty by offering wearable devices that are convenient to use. Wearables can be co-branded with a financial institution and leverage the benefits of marketing and loyalty comparable to those of the financial institution partners. Merchants may also introduce product branding opportunities via sponsorships and promotions.

An additional wearables use case for merchants and issuers is to build consumer-engagement programs combined with quality of living and products/services being offered. For example, fitness tracking and nutrition or activities rewards programs can be consolidated into a wearable's functionality along with payment.

Prepaid Program Managers/Event Organizers. Program managers are a category of issuing entities that can work in partnership with financial institutions to drive cashless consumer payment experiences in single or season-long events or environments. Payment functionality can be combined with access control and ticketing to create a single device that delivers consumer-friendly, one-stop engagement. This can also drive consumer "stickiness" through fan loyalty, while using the device beyond the designated environment. This use case can further extend the life of the wearable and the use of the prepaid account.

Device Manufacturers/OEMs. Consumer-centric device manufacturers continually explore new desired features. Payment functionality has been a central focus for feature innovation for all of the major mobile handset manufacturers, and payment technology is now being propagated into wearable devices. Watches, fitness trackers and other connected devices compete for consumer preference. Payment functionality is proving to be of importance when consumers choose one device over another. In addition, new cross-functional experiences can be offered to the consumer by building in new use cases: for example, fitness bands with financial rewards. Wearable device manufacturers do not need to become experts in payment technology to implement payment functionality. Payment technology suppliers already offer white-label wearable payment solutions that can be easily integrated into an existing hardware and software wearable platform.

Types of Payment-Enabled Wearables

Wearables are typically implemented with one of two types of technologies and models: active connected wearables and passive wearables.

Active connected wearables can accept, produce or communicate dynamic content to the consumer and/or another device. Such wearables have both an ISO/IEC 14443 interface and another communications interface and have their own power source. These devices most often will have a Bluetooth or other wireless communication interface and are paired to a mobile device or communicate directly to the Internet via WiFi or cellular connectivity.

Active connected wearables are provisioned with payment credentials in real-time while facilitating additional functionality such as an information display to deliver content to consumers – either self-generated content (e.g., fitness tracking, geolocation) or over-the-air dynamic content.

Examples of active connected wearables include: powered watches with Android, Apple or other proprietary operating systems; fitness/activity/health trackers; special purpose devices such as location trackers. All active, connected wearables may be combined with payment functionality.

For payment-enabled functionality, *passive wearables* have no additional means for information delivery or communications, and rely entirely on the ISO/IEC 14443-enabled contactless interface to function. Passive devices do not have a power source of their own. Passive wearables may be provided to the consumer with a generic (prepaid) credential already loaded and activated and associated with the consumer before first use.

The technology available today does not limit passive wearables to be pre-enabled with payment credentials. Similar to traditional payment cards, passive wearables may be instantly issued in the field leveraging the contactless interface.

Examples of passive wearables are: wristbands; rings; universal "insertable" devices, like a SIM-sized card or other card break-

out piece which can be inserted into multiple end-form factors (for example with different forms of bands, band attachments or other accessories). Fully pre-assembled wristbands and wristbands with insertable card break-out pieces have their own advantages and disadvantages depending on the use case and application.

Conclusions

When implementing payment-enabled wearables, industry stakeholders should consider the following:

- How will the consumer be motivated to use the wearable for payment? Will there be sufficient acceptance points?
- What is the use case for the wearable? Who is the target customer and when, how and where is the wearable going to be used? Understanding the use case will help with the technology decisions.
- Who are the stakeholders that will be involved in manufacturing, provisioning, distributing and managing the wearable device? The stakeholders may have different roles depending on the application use case and technology model selected.
- What is the certification, testing and approval process? How does this process fit with the overall timeline required for the wearable project?
- How will the payment-enabled wearable lifecycle be managed? Identification of the industry partners needed to provision and manage the wearable during its lifecycle is critical.

Payment-enabled wearables offer new opportunities for wearable device manufacturers, service providers and the payments industry to offer consumers exciting new payment form factors. From improved convenience for consumers to increased loyalty and "brand stickiness" sought by device manufacturers and service providers, wearables deliver benefits to all stakeholders in the ecosystem.

References

[1] "Gartner Says Worldwide Wearable Device Sales to Grow 17 Percent in 2017," Gartner news release, Aug. 24, 2017

[2] "Here's What's Holding Back Wearable Payments," Business Insider, March 10, 2017

About this Article

This article is an extract from the Secure Technology Alliance Payments Council white paper, "Implementation Considerations for Contactless Payment-Enabled Wearables," published in October 2017. The white paper provides an educational resource on the wearables landscape focusing on ISO/IEC 14443/secure element-based implementations and discusses key considerations for implementing payments in wearables. Members contributing to the development of this white paper included: American Express; Cardtek US; Discover Financial Services; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Infineon Technologies; IQ Devices; Mastercard; Metropolitan Transportation Authority (MTA); Multos International; NXP Semiconductors

Updates from the Alliance Industry Councils

Access Control Council

- The Access Control Council launched its new webinar series on PIV-enabled PACS implementation for government physical security specialists. The first webinar, "How to Plan, Procure and Deploy a PIV-Enabled PACS: Part 1," was held on October 19 and featured Michael Kelley (Parsons), Lars Suneborn (Secure Technology Alliance), Randy Vanderhoof (Secure Technology Alliance), and William Windor (DHS) as speakers. The second webinar, "Facility Characterization and Risk Assessment," will be held on November 30
- The Council updated its charter to align with the expanded Secure Technology Alliance mission. The updated charter focuses on accelerating the widespread acceptance, use, and application of secure technologies in various physical and digital form factors for physical and logical access control as applicable to both persons and non-person entities

Health and Human Services Council

- The Council has one active project: a webinar based on the concepts in the Healthcare 2.0: A New Paradigm for a Secure and Streamlined Healthcare Industry infographic published in 2016

Identity Council

- The Identity Council is working on a new white paper on the mobile identity landscape. The white paper will assess the market landscape, document use cases and identify best practices and requirements for industry

Internet of Things Security Council

- The Internet of Things (IoT) Security Council published a new white paper, "IoT and Payments: Current Market Landscape." The white paper outlines the current market landscape for implementing payments with IoT devices and provides guidance for developing IoT applications that will include payment. Members contributing to the development of this white paper included: American Express; Cardtek; Consult Hyperion; CPI Card Group; Discover Financial Services; Entrust Datacard; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Ingenico; Initiative for Open Authentication (OATH); IQ Devices; Mastercard; Metropolitan Transportation Commission (MTC); NextGen ID; NXP Semiconductors; Rambus; Underwriters Laboratories (UL); Visa
- The Council held a well-attended joint council meeting with the Payments Council and Mobile Council at the IoT Payments 2017 event. During the meeting, Council members brainstormed priorities for new projects

Mobile Council

- The Mobile Council is working on one white paper – Trusted Execution Environment (TEE) 101

Payments Council

- The Payments Council published the new white paper, "Implementation Considerations for Contactless Payment-Enabled Wearables." The white paper provides an educational resource on the wearables landscape focusing on ISO/IEC 14443/secure element-based implementations and discusses key considerations for implementing payments in wearables. Members contributing to the development of this white paper included: American Express; Cardtek US; Discover Financial Services; G+D Mobile Security; Gemalto; GlobalPlatform; IDEMIA; Infineon Technologies; IQ Devices; Mastercard; Metropolitan Transportation Authority (MTA); Multos International; NXP Semiconductors
- The Payments Council is working on two white papers – EMV contactless challenges/solutions for issuers, merchants and processors; EMVCo Payment Account Reference (PAR) use cases – and is collaborating with the U.S. Payments Forum on a white paper on approaches to secure the card-not-present environment

Transportation Council

- The Transportation Council currently has two active projects: a webinar on mobile ticketing and Near Field Communications (NFC); part two of the payments convergence white paper, focusing on potential barriers to implementation of multimodal payment strategies and suggesting ways of addressing these challenges

Other Council Information

- Secure Technology Alliance members are now able to request guest participation in U.S. Payments Forum projects. The list of active Forum projects is available on the Alliance member web site. If you would like to participate in one of the Forum projects, please contact Mike Strock. A list of active Secure Technology Alliance Council projects is also available to promote cross-council participation.
- If you are interested in forming or participating in an Alliance council, contact Cathy Medich.

Alliance Members: Participation in all current councils is open to any Secure Technology Alliance member who wishes to contribute to the council projects. If you are interested in forming or participating in an Alliance council, contact Cathy Medich.

Welcome New Members

- Elavon, Leadership Council PLUS member
- RF IDeas, General member

New Certification Recipients

CSEIP

- Dan Burnell, Convergint Technologies
- Jon Bybee, Parsons Corporation
- Sean Eaton, Johnson Controls
- Eric Eddy, Johnson Controls
- Edgar Freeze, Security Install Solutions
- Jason Greenwood, HEI Security
- Jose Hernadez, OmniTech Services
- Eric Johnson, U.S. Marshal Service
- Richard McGinnis, Security Install Solutions
- Barry Mims, OmniTech Services
- Scott O'Neal, Johnson Controls
- Tom Owens, E2 Optics
- Cheri Pool, Integrated Environments
- Sean Reynolds, U.S. Marshal Services
- Richard Shafer, Xpect Solutions
- Brandon Sutphin, Johnson Controls
- Jasen Vonheeder, MEI Systems Integrators

Secure Technology Alliance In The News

"Why wearable payments need one-size-fits-all security." Payments Source. In this feature article, Executive Director Randy Vanderhoof explains why it's vital that the security woven into wearables is consistent and clear, particularly for payments applications.

"Tickets? Puh-leez. There Are Lots of New Ways to Pay Bus and Train Fares." Governing. Executive Director Vanderhoof tells Governing that transit agencies are moving away from the proprietary systems they used in the past and adopting standards that are used "everywhere" outside of transit.

For more information, visit our website at www.securetechalliance.org. Members can also access white papers, educational resources and other content.

SECURE TECHNOLOGY ALLIANCE
191 Clarksville Road
Princeton Junction, New Jersey 08550
1.800.556.6828
Fax: 1.609.799.7032
info@securetechalliance.org
www.securetechalliance.org

About Secure Tech Talk

Secure Tech Talk is the monthly e-newsletter published by the Secure Technology Alliance to report on industry news, information and events and to provide highlights of Alliance activities and membership.

About the Secure Technology Alliance

The Secure Technology Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption and widespread application of secure solutions, including smart cards, embedded chip technology, and related hardware and software across a variety of markets including authentication, commerce and Internet of Things (IoT).