black hat USA 2020
AUGUST 5-6, 2020
BRIEFINGS

Building a Vulnerability Disclosure Program That Works for Election Vendors and Hackers

Synack

Mark Kuhr
CTO, Synack

Chris Wlaschin
VP, Systems Security and CISO, ES&S

ES&S ELECTION Systems & Software

Chris Wlaschin

VP Systems Security and CISO, ES&S

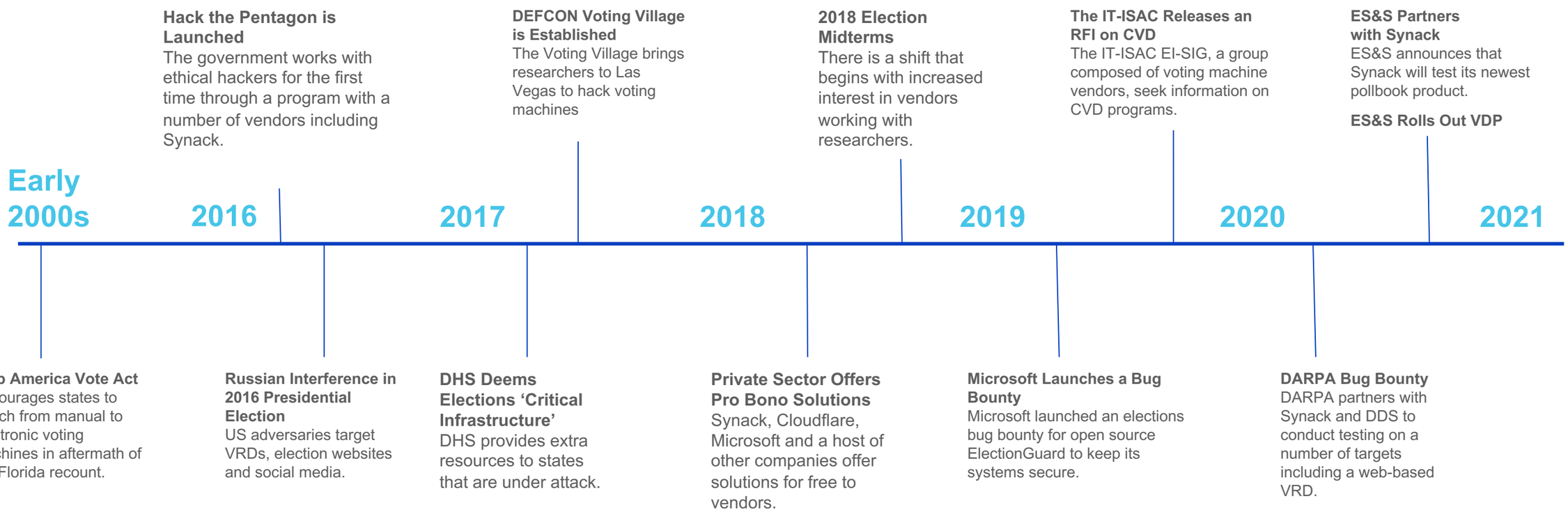
- Former CISO for HHS
- Deputy CISO for the VA
- Director of Security for
  National Research Corporation
- CISO for the University of Nebraska
- CIO for the Military Sealift Command
- Chief of Operations for the Defense Intelligence Agency
  Western Region
- 20+ years U.S. Navy

Dr. Mark Kuhr

CTO, Synack

- Dr. Mark Kuhr is the CTO and Co-Founder of Synack, the leader of crowdsourced security
- Former NSA exploitation analyst/operator
- DISA Command & Control Systems Engineer
- Ph.D. in Computer Science from Auburn University under a DoD/NSA-sponsored fellowship

The State of Election Security is Improving



Crowdsourced Security Models for Collaboration between Security Researchers and the Vendors, State/Local and Federal Government

Vulnerability Disclosure Program

- Basic policy and process for public disclosure of known vulnerabilities

Open Bug Bounty

- Basic coverage for unknown vulnerabilities
- Live hacking events

Invite-Only Bug Bounty

- Selected Crowd
- Continuous testing option with humans

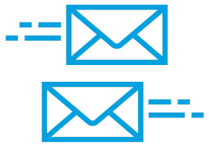
Managed Crowdsourced Penetration Testing

- Adversarial testing coverage
- Vetting crowd
- Continuous testing with humans and vendor provided AI/MC scanner option
- Live hacking events
- Coverage data and analytics
- Auditability/Tracking
- Risk Scores

VDP at ES&S

Internal vulnerability assessment process in place

- Determination of applicability and risk essential to resource allocation
- Product and Certification Teams are critical to success



Communication channel in place

- security@essvote.com
- Used externally and internally to report vulnerabilities and ask questions

Collaboration with researchers is working

Crowdsourced Pen Testing at the State Level

“The State of Colorado considers considers pen testing, and Synack’s crowdsourced pen testing specifically, as a crucial part of a cybersecurity program.”

- Colorado Secretary of State CIO, Trevor Timmons

Example #1
Citrix NetScaler

Researcher Jack Cable

Vulnerability Citrix NetScaler VPN appliance susceptible to malware CVE-2019-19781

- Discovered by Synack SRT member in Dec 2019
- Malicious file upload leads to full compromise of devices
- How long was this known by the adversary?

Methodology Make a request to `GET /vpn/../vpns/cfg/smb.conf` (note that this should be done in a proxy such as Burp Suite in order to execute the raw request).

Example #1
Citrix NetScaler

Evaluation

Directory traversal vulnerability is caused by improper handling of the pathname. Lacking a data sanitation check the system uses the path in incoming requests directly. Requests containing a path like /vane/../vpns/services.html, are transformed into simply /vpns/. This vulnerability in the system could allow remote attackers to exploit directory traversal requests and access sensitive files without the need for user authentication.

Mitigation

Apply a specific responder policy to filter exploitation attempts.

Example #2
Firewall Ports and Protocols

Researchers Kevin Skoglund, Tony Adams

Vulnerability Ports 22 and 443 can fingerprint firewalls used in unofficial results reporting. https_//nvd.nist.gov/vuln/detail/ CVE-2018-0101

Methodology https://censys.io/ipv4?q=22.ssh.v2.metadata.product%3ACerberusFTPServer+AND+metadata.manufacturer%3ACisco

Evaluation Without proper security controls, misconfigured or unfiltered internet-facing services may be abused by opportunistic or targeted malicious threat actors.

Mitigation ES&S system hardening scripts and https_://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf

Example #3
Zebra Scanners

Researchers	Kevin Skoglund, Tony Adams
Vulnerability	Zebra scanners/printers shipped from OEM with unrestricted end-user access to front panel options. CVE-2019-10960
Methodology	In-depth review of EAC certification test plans for ES&S certification documentation lists COTS Hardware which includes: "Zebra Technologies, QR code scanner (Integrated), DS457-SR20009.

Example #3
Zebra Scanners

Evaluation

Configuration barcodes are special, manufacturer-defined barcodes which can be scanned by a scanner to change:

- Scanner's settings
- Types of barcodes the scanner reads
- How it reads barcodes
- How it processes barcodes

Mitigation

ES&S' use of the Zebra devices includes Skoglund's recommendation that voting system software should:

- Thoroughly sanitize all data received via a barcode scanner to prevent code injection
- Consider and securely handle all input, even unexpected commands

Example #4
VoterView Look

Researcher	Hunter Osmera
Vulnerability	VoterView application responds to random character input in name fields returning voter directory information
Methodology	Manual and bot-based random character injection into the data fields of the voter lookup website

Example #4
VoterView Look

Evaluation

Special characters are being ignored by the search parameter and the application is treating the subsequent blank first name and blank last name as not part of the search, then using only the date of birth as the search criteria, thus returning multiple voters with the same birthdate.

Mitigation

Software updated to prevent exploitation of random character injections by disallowing special characters that are unlikely to appear in names.

Secure the Election

Security by America for America

The best security is rooted in a united effort. Synack's Secure the Election initiative provides pro bono crowdsourced security testing and vulnerability disclosure programs to states prior to the 2020 Presidential Election. Synack believes that hackers can provide an adversarial perspective on where states are vulnerable. A "see something, see say something" policy as well as rigorous crowdsourced pentesting are best practices and will deter future attacks.

Services include:

- Which servers are connected to the internet?
- Do online voter registration sites connect to the VRDB?
- Can admin access be gained? Can accounts be edited?
- Can the VRDB be accessed through a 3rd party system?

The Result: finding & fixing vulnerabilities before exploitation

The Future of Electronic Security & Elections: FETT Bug Bounty with DARPA, DDS, and Synack

DARPA FETT (Finding Exploits to Thwart Tampering)

- DARPA is hosting the Finding Exploits to Thwart Tampering (FETT) Bug Bounty – a crowdsourced pentesting exercise that aims to evaluate the hardware architectures in development on the SSITH program with the goal of uncovering and addressing potential bugs and vulnerabilities.

DARPA is doing research on how to harden electronic systems including, including VRD

- Voter registration systems are something that each U.S. county and state must stand-up on their own. There are few, if any, standards guiding these systems and they utilize the same web servers and database back-ends as many other internet-enabled systems.
- DARPA felt that the SSITH hardware defenses could help protect these systems from certain attacks and believe the issue to be increasingly urgent.

Specific Software Vulns that Create Issues in Hardware (Source: DARPA)

DARPA has focused on security research to protect against the following vulnerability classes that occur in electronic systems, including Voter Registration Databases (VRD):

- Buffer errors
- Information leakage
- Permissions, Privileges, Access Control
- Numeric errors
- Resource management
- Code Injection
- Crypto Errors

Next Steps

The IT-ISAC EI-SIG has formed an Advisory Committee on Coordinated Vuln Disclosure (CVD) which is driving toward industry-wide VDP.

ES&S is partnering with Synack to test its newest generation pollbook.

Next Steps

The Federal Testing Program needs tweaking to allow for quick testing.

- Testing timelines are currently too elongated for a full CVDP
- Incorporation into federal certification standards

Customers (state and local election officials) benefit

- Increased confidence in systems and software
- Public awareness improves overall impression of election tech

Supply Chain Security Considerations

ES&S Product Life Cycle

Sustainability & Supply Chain Security

1. Product Requirements
2. Design & Vendor Selection
3. Development & Quality Assurance
4. Certification & Compliance
5. ISO Manufacturing, Incoming Inspection, QC, Order Fulfillment & Implementation, Repeatable Processes
6. Sustainable Engineering, Customer Support & EOL

Supply Chain Security Considerations

- As is the case with many critical infrastructure sectors, ES&S has certain global supply chain dependencies.
- ES&S' Engineering Team continually reviews the ability to source components within the U.S. Some components are:
  - Sole-sourced
  - Protected by a patent
  - Intricate to the design of the circuit or sub-assembly
  - Not able to be procured from alternative suppliers
- ES&S' experts evaluate the risk and impact of using those components and assess safeguards to limit risk when using sensitive components.
- Every aspect of our system is under a secure Engineering Change Order (ECO) control process, regardless of where individual components are produced.

Supply Chain Security Considerations

ES&S conducts thorough security reviews of its supply chain to ensure every component is trusted, tested and free of defects, including:

- Risk assessments using NIST Cybersecurity Framework (CSF) tools
- On-site visits to suppliers

Supply Chain Security Considerations

- These audits utilize both on-site quality teams, as well as site visits to confirm that contract manufacturers are following prescribed processes.
- ES&S contract manufacturers' procurement and supplier oversight policies are thoroughly vetted by ES&S to ensure they meet the established requirements.

Supply Chain Integrity

Once the hardware components are delivered to Omaha, ES&S performs several essential steps, including:

- Verification that the firmware on the PLDs within the hardware is exactly what it is expected it to be and not altered in any way
- Final hardware configuration
- Final end-to-end QC test which includes loading of the certified software and firmware

SCRM ESSENTIALS

Information and Communications Technology Supply Chain Risk Management (SCRM) in a Connected World

THE LEADER'S GUIDE

Protecting your organization's information in a digitally connected world demands an understanding of third-party vendor supplier security. Consider which organizations are in your supply chain and whether you trust the hardware, software, and services you receive. As with other risks, supply chain risks can threaten:

- YOUR ABILITY TO OPERATE/ACCESS INFO
- YOUR REPUTATION/CUSTOMER TRUST
- YOUR BOTTOM LINE
- YOUR ORGANIZATION'S RESILIENCE

Managing supply chain risks requires building an effective supply chain management practice and understanding extended supply chains that consist of suppliers, vendors, and service providers.

Essential Steps to Building an *Effective Supply Chain Risk Management Practice:*

Step 1 — Identify *- The People*

Determine who from your organization needs to be involved

Build a team of representatives from various roles and functions of the company (e.g., cybersecurity, information technology, physical security, procurement/acquisition, legal, logistics, marketing, and product development). Ensure personnel at all levels are well-trained in the security procedures of their role or function.

This team will bring together diverse perspectives of subject matter experts from across your organization.

Step 2 — Manage *- The Security and Compliance*

Develop your supply chain security policies and procedures

Document the set of policies and procedures that address security, integrity, resilience and quality. Ensure they are based on industry standards and best practices on how to conduct supply chain risk management, such as those from the National Institute of Standards and Technology (NIST).[1]

Promote a leadership-encouraged culture of supply chain readiness.

Step 3 — Assess *- The Components*

Understand the hardware, software, and services that you procure

Build a list of the information and communications technology (ICT) components (e.g., hardware, software, services) that your organization procures to enable your business. Know which internal systems are relied upon for critical information or functions, and which systems have remote access capability that must be protected to prevent unauthorized access.

Step 4 — Know *- The Supply Chain and Suppliers*

Map your supply chain to better understand what components you procure

Identify your suppliers and, when possible, the suppliers' sources. In today's world of increased outsourcing, it is important to understand your upstream suppliers as part of the larger supply chain ecosystem.

Consider suppliers of critical components as well as those that provide assets, systems, and data that enable your business.

Step 5 — Verify *- The Assurance of Third Parties*

Determine how your organization will assess the security culture of suppliers

Verify that your suppliers maintain an adequate security culture and supply chain risk management program to appropriately address the risks that concern your organization. Establish the protocols your organization will use to assess the supply chain practices of your suppliers.

Consider the types of frameworks, models, qualification criteria, contractual clauses and monitoring you will use to assure trusted supply chain practices.

Step 6 — Evaluate *- The Review*

Establish timeframes and systems for checking supply chain practices against guidelines

Determine the frequency with which you will review your SCRM program, incorporate feedback, and make changes to your risk management program. This may also include auditing suppliers against practices and protocols established by your organization.

Your supply chain risk management program will continuously move through these steps.

[1] To learn more about SCRM-related key practices (e.g., NIST SP800-161, NISTIR 8276), news, and latest projects, visit the NIST's webpage at **https://csrc.nist.gov/Topics/Security-and-Privacy/supply-chain**.

www.CISA.gov/NRMC-SCRM

flip page ▶

Questions?