The Secret to Secrets Management

The modern IT landscape is filled with secrets: certificates, cryptocurrency wallets, SQL connection strings, storage account keys, passwords, and encryption keys. A centralized approach to secrets management is vital to protect data and assets, whereby poorly-managed security could lead to breach, non-compliance, or outage.

Mark B. Cooper, president and founder, PKI Solutions

Cooper is known as “The PKI Guy” since his early days at Microsoft. He has deep knowledge and experience in all things Public Key Infrastructure (PKI). PKI Solutions Inc. provides consulting, training — including online training — and implements software solutions for Microsoft PKI and related technologies at enterprises around the world.

To ask a question, use the green “**Q&A**” button on the left side of your screen. All questions are anonymous.

CyberRisk Alliance | Business Intelligence Resources

PKI SOLUTIONS

Today's Speaker

Mark B. Cooper

President & Founder

PKI Solutions

Mark@PKISolutions.com

@ThePKIGuy

Agenda

- Current IT/cyber landscape
- Defining secrets
- How to get a handle on secrets management
- Know where secrets are kept
- The pitfalls of poor secrets management
- Set your goal
- Levels of security
- How to centralize your approach
- Administration vs. technology solutions
- Questions

The PKI Guy

- President and Founder, PKI Solutions
- Known as “The PKI Guy” since early days at Microsoft
- At PKI Solutions, we implement PKI solutions at enterprises
- I lead hundreds of PKI trainings from Scotland to Buffalo, Sweden to Portland
- In-person and online training available
- My focus is security, PKI design and implementation, identity management

What Are We Talking About Today?

- An introduction to secrets management
- Understand how to separate data from the secrets/keys that protect this data
- Learn specific ways for organizations to better store, manage, and protect their secrets
- Learn how to and not to handle secrets

Current IT/Cyber Landscape

"Cybersecurity is the biggest threat to the global economy."

- EY 2019 CEO Imperative Study

- 43% of businesses were a victim of a cybersecurity breach last year
  - Cyber Security Breaches Survey 2018
- Compromising secrets is one of the top ways of hacking a system.
  - CNBC
- 80% of data breaches are caused by silly mistakes by those responsible for managing secrets.
  - Rashmi Jha, Microsoft
- 87% of executives lack confidence in their organization's level of cybersecurity.
  - EY

What is a Secret?

"A secret is some knowledge, or piece of data, that is hidden from entities. A secret is what is needed to access your applications, services, and IT resources."

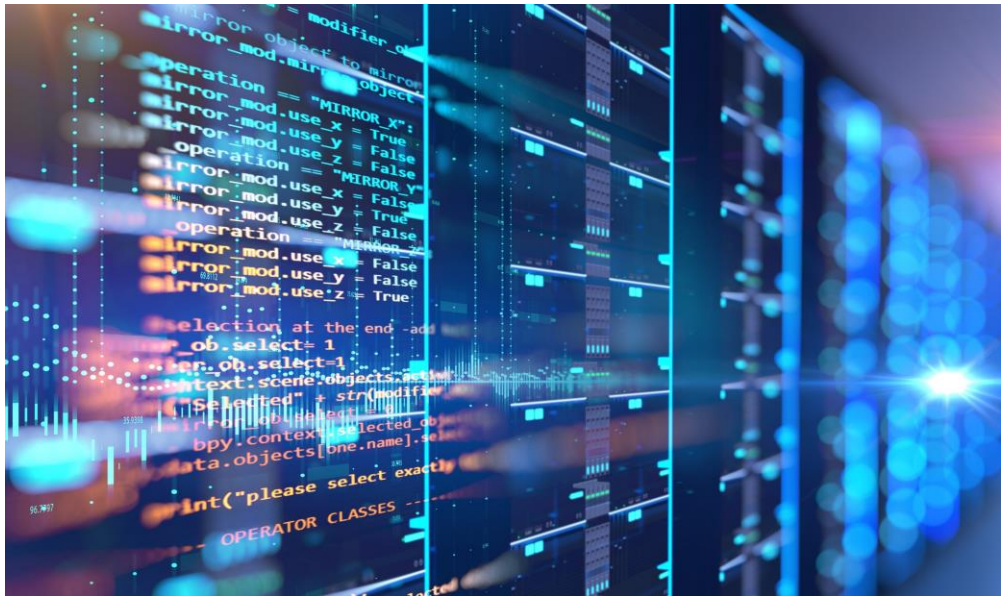
- Passwords
- Encryption Keys
- Symmetric
- Asymmetric (Private)
- Cryptocurrency wallets
- SQL connection strings
- Storage account keys
- API Tokens

How to Get a Handle on Secrets Management

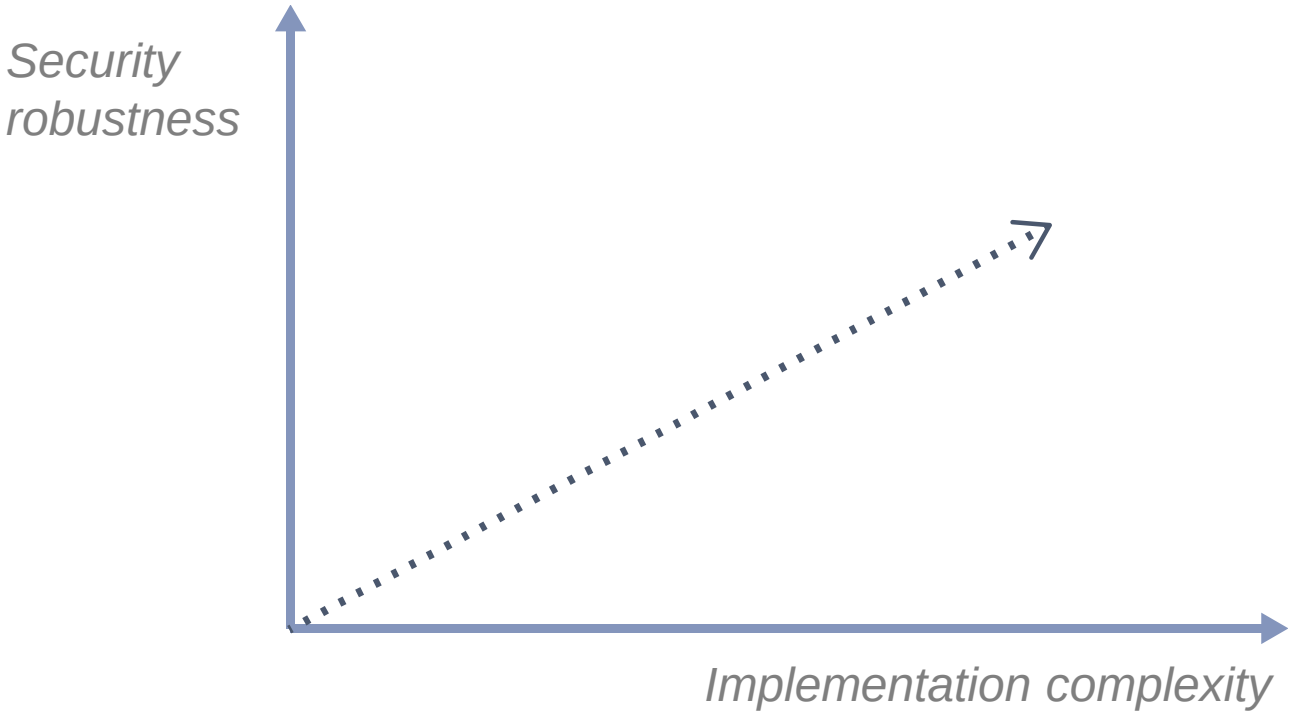
- Inventory the secrets; know where secrets are kept
- Fragmented approach; need to centralize
- Control access
- Remove human factor if possible (escrow services)
- Check permissions: users, machines, applications
- Log use and look for patterns
- Rotate keys regularly
- Plan ahead for data breach to reduce the impact
- Incident response

Know Where Secrets Are Kept

- Easier said than done! Often scattered
  - On premise
  - Cloud
  - Servers
  - Devices
  - Clients
  - In code – Ugh!
- Application support and dependencies



Set Your Goal



CyberRisk Alliance | Business Intelligence Resources

PKI SOLUTIONS

The Carrot or the Stick

- Will secret management be defined by your vendors?
- Application support common denominator defining your highest achievable bar
- Vendors indirectly dictate your security posture
- Define your own secret management goals
- Establish baseline standard for today (map to existing apps if needed)
- Create 2-5 year goal for your security standard
- Vendors are notified they must support that standard or face replacement
- New RFP and application selection criteria will factor in new requirements before acquisition

Levels of Security

- Limited access: secrets are stored in a repository/server with limited access to the public.
  - Password Vaults
  - Hardware Security Modules
  - Private git repository
- Encrypted secrets: before being stored, the secrets are encrypted
  - Security through obscurity is not acceptable.
- Management: an application that allows high level control of the secrets
  - Symmetric Key Management Systems
  - Password Escrow Services

The Pitfalls of Poor Secrets Management

- Account compromise
- Network compromise
- Information leak
- Data breach
- Outages
- Compliance issues
- Loss of reputation
- Business shutting down

How to Centralize Your Approach

- Place secrets in private repository
- Central
- Restricted access
- Separate data from secrets/keys
  - Use location to your advantage. Secrets on premises, data in the cloud
- Keep data encrypted using keys
- Ensure keys are encrypted at rest

Administration vs. Technology Solutions

- Human element will always be the weakest
  - Leverage escrow services when passwords are involved
  - Consider alternate identity solutions in-lieu of passwords
- Trust but verify
  - Key Management solutions are only part of the equation
  - Audit, Compliance, and Remediation are critical
  - Ongoing effort
- Consider security around any centralized repository
  - Guess who else is going to be interested in it?

Solutions Available Today

- Public Key Infrastructure
- Password Vaults – CyberArk
- Key Management Systems – Vormetric, Cryptomathic
- Microsoft SQL TDE, Always Encrypted
- Azure Key Vault

CyberRisk Alliance | Business Intelligence Resources

PKI SOLUTIONS

Online PKI Training: Discount for Attendees

- Online Microsoft PKI In-Depth Course, taught by Mark B. Cooper
- 20 hours of content + labs, self-paced
- https://www.pkisolutions.com/online-courses/
- Participants in today's conference: enter the code "CyberRisk" for 20% off this online course, valid until October 31, 2019

QUESTIONS?

THANK YOU FOR JOINING US!

Mark B. Cooper, president and founder, PKI Solutions

Please send any feedback or questions about today's presentation to customerservice@misti.com.