Countering Attacks From The Digital Horde

Dave Lewis
Global Advisory CISO
Cisco Systems
@gattaca
WHOAMI

RESEMBLANCE?
hackers must have tools
hackers must know
hackers must read books
hackers must die
hackers must have apps
hackers must be stopped
why hackers must eject the sjws
ethical hackers must obtain
all hackers must die
movies that hackers must watch
Securing the Enterprise

Access happens everywhere – how do you get visibility & ensure secure, trusted access?

**Workforce**
- All Corp IT
- User & Device Access

**Workload**
- Data Center
- Apps
- Servers
- Databases
- Application & Workload Access

**Workplace**
- Corporate Network
- Network Traffic
- Wireless
- IoT Devices
- User & Devices
- Network Access
Know Thyself...
Educational Programs

SECURITY AWARENESS
Audit All The Things!

- Testing your breach incident response plan
- Risks and benefits of information sharing
- Often Compliance is the adult in the room
The Risk Register
Encrypt Your Data
Backup, Backup, Backup...and Test Them
Defined Repeatable Process
Patch Management
Time To Say Goodbye To Passwords
Multifactor Authentication

1. LOG IN WITH SMARTPHONE
   - USER@EMAIL.COM
   - LOG IN

2. LOCAL DEVICE AUTHENTICATION
   - Fingerprint

3. COMPLETE
WebAuthn
Authenticating with a WebAuthn Credential

After registration has finished, the user can now be authenticated. During authentication an assertion is created, which is proof that the user has possession of the private key. This assertion contains a signature created using the private key. The server uses the public key retrieved during registration to verify this signature.
Verification will look different depending on the language and cryptography library used on the server. However, the general procedure remains the same.

```javascript
const storedCredential = await getCredentialFromDatabase(userHandle, credentialId);

const signedData = (authenticatorDataBytes + hashedClientDataJSON);

const signatureIsValid = storedCredential.publicKey.verify(signature, signedData);

if (signatureIsValid) {
    return "Hooray! User is authenticated! 😊";
} else {
    return "Verification failed. 😞";
}
```
WebAuthn.io
A demo of the WebAuthn specification
• Do you really need that data?
• Is that data encrypted?
• Is the data safely controlled?
• Roll out a retention policy.
Cross Organizational Teams
Protect The Workforce
Protect The Workload
Protect The Workplace
Threats Today, As a Result

A new approach to security is needed – zero trust – to address identity, app & network threats.

Targeting Identity
81% of breaches involved compromised credentials

Targeting Apps
54% of web app vulnerabilities have a public exploit available

Targeting Network
92% of external pentests led to a breach of network perimeters
We Must Adapt
Business Challenges

Increased complexity, attack surface & gaps in visibility

Excessive Trust

- How do we know users are who they say they are?
- Are their devices secure & up to date?
- What’s on the network? How does it connect?
- What data’s in the cloud? Who/what accesses it?
- How can we view & secure all connections?
- What exists in the cloud? How does it connect?
Businesses Must Understand Their Supply Chain
Supply Chain
Heist

In Hours, Thieves Took $45 Million in A.T.M. Scheme

By MARC SANTORA
Published: May 9, 2013

It was a brazen bank heist, but a 21st-century version in which the criminals never wore ski masks, threatened a teller or set foot in a vault.

In two precision operations that involved people in more than two dozen countries acting in close coordination and with surgical precision, thieves stole $45 million from thousands of A.T.M.'s in a matter of hours.

In New York City alone, the thieves responsible for A.T.M. withdrawals struck 2,904 machines over 10 hours starting on Feb. 19, withdrawing $2.4 million.

The operation included sophisticated computer experts operating in the shadowy world of Internet hacking, manipulating financial information with the stroke of a few keys, as well as common street criminals, who used that information to loot the automated teller machines.
New York
The Flow

[Diagram of payment flow]
The Penetration Test
Stepping Stone to Compromising High Value Target
Strategically Think About Securing Business

1. Confirm User Identities
2. Ensure Device Security
3. Enforce Contextual Access Policies
4. Secure Access to All Applications
5. Gain Access Visibility
Digital Transformation & SRE
Attackers Will Improvise
Return To Core Fundamentals
Apply What You Have Learned Today

- Next week you should:
  - Identify critical assets, users and applications within your organization

- In the first three months following this presentation you should:
  - Have a clearly defined risk register
  - Define appropriate controls to move towards a zero trust landscape.

- Within six months you should:
  - Begin a project to move towards a zero trust model.
  - Drive an implementation project to reduce risk in your environment.
Thanks for listening!

gattaca@cisco.com
@gattaca