Security Engineering

Supply Chain Attacks: Operation Gunman
Supply Chain Attacks (2): Cisco Routers
Supply Chain Attacks (3): Supermicro Motherboards

• Chip implanted into the motherboard to “phone home”

• Implant not placed in Supermicro’s design, but altered at manufacture time!

• Is this easier than bugging the software? Or the BIOS (also hacked in this instance)?

• Who along the supply chain could get you? It’s not always the easiest targets, but the most accessible.
Platform Security

Who is in charge?

- Mobile Network Operator (MNO)
- Handset Original Equipment Manufacturer (OEM)
- OS Vendor
- Chip Maker
- Chip Designer
Platform Security: Android

<table>
<thead>
<tr>
<th>Role</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Network Operator (MNO)</td>
<td>EE</td>
</tr>
<tr>
<td>Handset Original Equipment Manufacturer (OEM)</td>
<td>HTC</td>
</tr>
<tr>
<td>OS Vendor</td>
<td>Google</td>
</tr>
<tr>
<td>Chip Maker</td>
<td>TSMC</td>
</tr>
<tr>
<td>Chip Designer</td>
<td>Qualcomm &amp; ARM</td>
</tr>
</tbody>
</table>

How do updates Propagate?
Why is Android Free?
Platform Security: Apple

<table>
<thead>
<tr>
<th>Mobile Network Operator (MNO)</th>
<th>EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handset Original Equipment Manufacturer (OEM)</td>
<td>Apple</td>
</tr>
<tr>
<td>OS Vendor</td>
<td>Apple</td>
</tr>
<tr>
<td>Chip Maker</td>
<td>TSMC/Samsung</td>
</tr>
<tr>
<td>Chip Designer</td>
<td>Apple &amp; ARM</td>
</tr>
</tbody>
</table>
Platform Security: Apple

- WiFi
- 4g connection
- USB to iTunes
App Store Ecosystems
App Store Ecosystems
Pokémon UNITE
The Pokémon Company
In-app purchases

4.2 ★
337K reviews
10M+ Downloads
PEGI 3

Install

About this game
5-on-5 Strategic Team Pokémon Battles!

#1 top free in action

Ratings and reviews

Boss Life 3D
Alictus
Contains ads

3.6 ★
2K reviews
1M+ Downloads
PEGI 12

Install

About this game
Be the best boss ever!

#1 top free in casual Simulation

Ratings and reviews
## App Store Ecosystems

<table>
<thead>
<tr>
<th>Mobile Network Operator (MNO)</th>
<th>EE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Handset Original Equipment Manufacturer (OEM)</td>
<td>HTC</td>
</tr>
<tr>
<td>OS Vendor</td>
<td>Google</td>
</tr>
</tbody>
</table>
Google Play

Manage apps and device

Overview

No harmful apps found
Play Protect scanned at 09:34

Updates available
8 updates pending
Update all
See details

Share apps
Send
Receive

Ratings and reviews

Pending downloads

Apps (8)

Android Accessibility
29 MB • Updated on 2...
Update

Facebook
52 MB • Updated 4 da...
Update

Google Home
17 MB • Updated on 2...
Update

Google Maps
30 MB • Updated at 0...
Update

Microsoft SwiftKey K...
9.5 MB • Updated on...
Update

NHS COVID-19
8 MB • Updated on 1...
Update

WhatsApp Messenger
17 MB • Updated on 1...
Update
Google Play (2)

• Self-signed applications (unlike iOS)
• Default with no “Install Apps from External Sources” – security and lock-in
• App Security Improvement Program
Google App Security

• Suite of Sanitizers and Mitigators for User Code: BoundsSan, AddrSan, IntSan, Shadow Stacks, Scudo
  Hardened Allocator

• Not just about protecting Android the OS: if you extract rent from an ecosystem, you need to protect the 3rd party code too!
Android Security Updates

 festivities
Android Update Lifecycle

1. Android Dessert Release
2. Board Support Package
3. Device Makers
   - Customize with their own & carrier requirements
4. Carriers
   - Device makers seek technical acceptance (TA)
5. End Users

Android Update Lifecycle

Before Treble

Android Update Lifecycle

With Treble

Android Update Lifecycle: Project Mainline

Other Android App Security Mechanisms

- From the Chip Vendor: TrustZone.
- Obfuscation: mandatory in banking.
- Android KeyStore
- SIM locking: device in the custody of the attacker!
Apple

• (Semi)-closed ecosystem.
• 30% commission on products sold through App Store, incl. IAPs – antitrust issues e.g. Epic Games Lawsuit
• Patches for 5ish years – why does Apple have more incentive here?
• Largely closed source – there is obscurity, but is it part of the security?
Apple IDFA

“Pal About” would like permission to track you across apps and websites owned by other companies. Your data will be used to deliver personalized ads to you.

Allow Tracking

Ask App Not to Track
App Ecosystem (Continued)

• Apps can be/go bad for many reasons.
• “We Purchase Apps” – ad fraud.
• Tussles around trust in Ad Networks even in reputable apps: e.g. CamScanner started dropping Trojans on phones!
• Google: Apps assumed bad and contained. Windows: global visibility, with Antivirus to do the heavy lifting.
• Google Play Store still has trouble with “Repackaging”: adding “Riders” to “Carrier” apps.
“Why is Windows so Insecure?”

- Medical and defence can build dependable systems, so why was Win95/98 totally defenceless?
- “Ship it Tuesday and get it right by Version 3”.
- Competition for the market: rational to get as much (poorly written) software as quickly as possible.
- Initial vs Sustained Velocity, and Technical Debt
- “Bargains then Ripoffs” – not just poor security, but dumping costs on users also rational behaviour.
Microsoft “turned their s*** around”

• “I would always make a point of asking hackers, ‘I know you hate the vendors, but of all of them, who do you hate least?’ The answer was always the same. ‘Microsoft,’ they would tell me. ‘They turned their s*** around.’” – Nicole Perlroth

• From XP Onwards: free security tools, secure coding training for all staff, patching.

• BUT – more effort went into protecting premium video than credit card numbers!
Maturing your Ecosystem

• What might a patch to fix a bug break, in the Windows Software *Ecosystem*?
• ...With legacy code that likely assumes it’s running as admin?
• Sustained Velocity bites...
• Can you change your Ecosystem to make it more secure? Microsoft tried and failed with the Windows App Store, Universal Windows Apps, and Windows 10S.
• Is this all Microsoft’s fault? Why target OSX when Windows has 5x the users...
Azure

• Microsoft moving to a new ecosystem... the CLOUD.
• Not just about using Microsoft’s Server Hardware – also about using their software ecosystem.
• Azure Security Centre: Compliance reporting, threat modelling, crypto standards, managing risks of 3rd-party components, pen testing.
• “Bargains then Ripoffs”
Azure - Encryption

• HSMs now maintained by Azure or Amazon, not the bank!
• Double Encryption DRM
• Cloud Key vault
Code Supply Chain

• Can insiders (un)intentionally get bad code committed to release?

• Who is an “insider” for the software running in your device? Think about your OS kernel, libraries...

• Code reviews are a form of multi-party authorisation, but be careful to avoid rubberstamping...

• In this scenario, bugs aren’t random – they’re introduced to open-source projects with wide use!
Code Supply Chain (2)

• Who makes the decision to integrate patches into your products?

• Third-party code review: keep an internal version and review upstream patches as they appear.

• The Compiler is part of your TCB!

• Code signing can help you work out provenance, but watch out for your keys leaking, and beware of who has signing keys...
Vulnerability Market Ecosystems

Discovered Bug

- Customer?
- Academic?
- User of Product?
- Intelligence Agency Contractor?
- Criminal?

Discovered for Free?

- Disclose to single company?
- Disclose to lots?

Bug-Bounty Program?

- Use on lots?
- Use on one target?

Vulnerability Market?

- Disclose to single company?
- Disclose to lots?

Cyber-Arms Manufacturer?

- Use on lots?
- Use on one target?

Exploit it Yourself?

- Sue you?
Whose Fault is it Anyway?

• Incentives are to blame shift – both to partners in your ecosystem, and even within teams in the same company.

• Your hardware teams will blame your software teams: who should actually fix it?

• BIDI attacks: Compiler? Editor? Build environment? Repository code-smell checking? The easiest deployment may not be the cheapest or most comprehensive...
Accessory Control
Razors and Blades Model

- Two-part pricing.
- Lexmark vs SCC 2004: free market for cryptologists!
Example: Nintendo

Developer

Consumer

DRM

Challenge-response

Code signing
Example: Overrun Prevention

- Accessory Control gets complicated with complex supply chains
- E.g. you’re an IP vendor selling a circuit design to be run on cameras at $2 per camera.
- You sell licenses for 100k cameras, and find 200k appear on the market.
- IP Vendor -> Camera Company -> Factory. Who has incentives to cheat?
Is Accessory Control Objectionable?

• Depends how competitive the markets are.
• BUT – tech entrenches and causes monopolies...
• Right-to-Repair Laws – a common battleground.
• Sustainability: accessory control usually lowers lifetimes.