



ISO 9001:2000 Certified

Teddy Bear Attack & Penetration

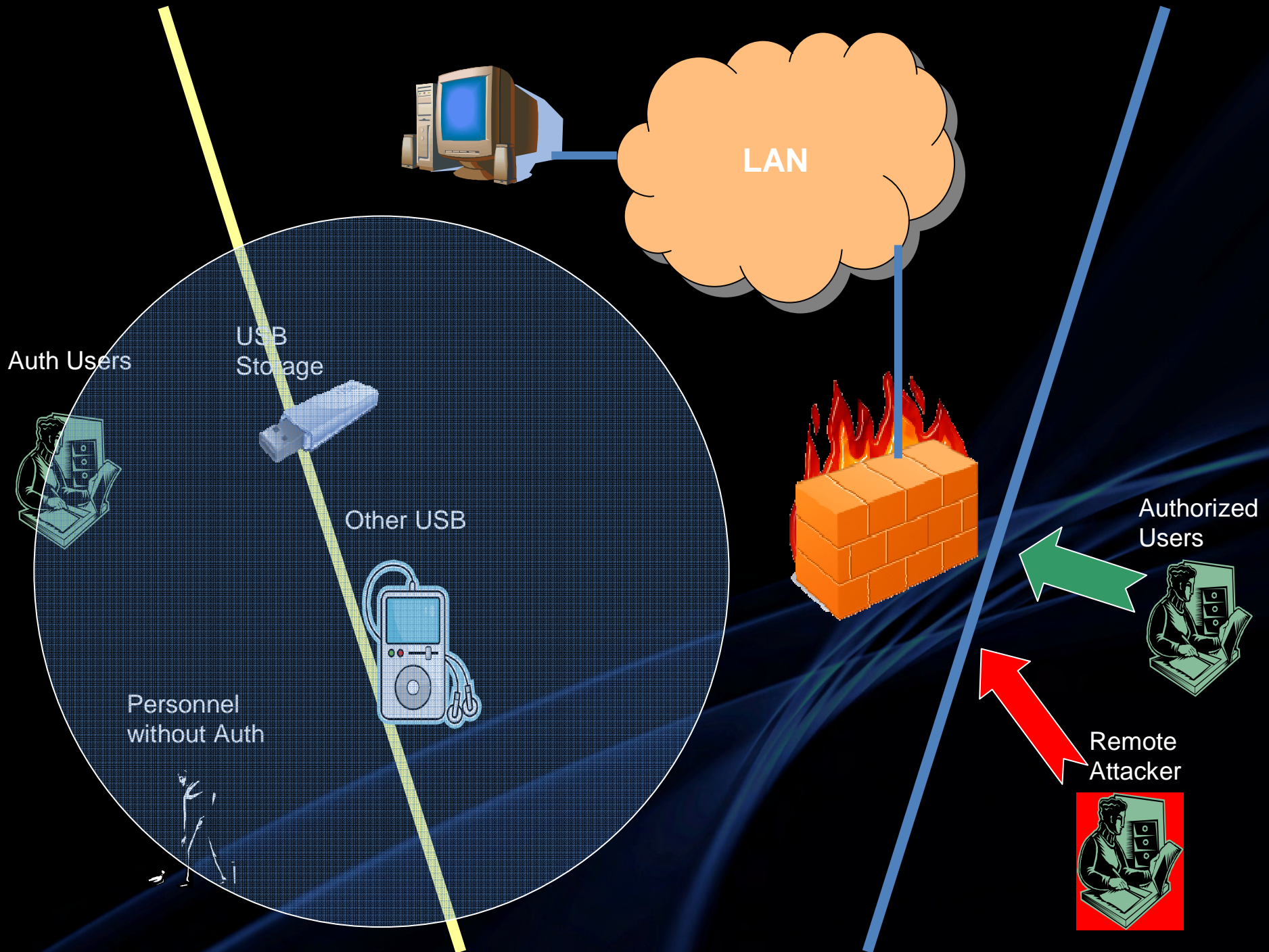
Weaponized USB as an Attack Vector

Steve Goldsby

Our Framework

- System & Network Boundary Review
- The Problem
- Demonstration
- Impacts to your Environment
- Mitigation Strategies
- Scenarios

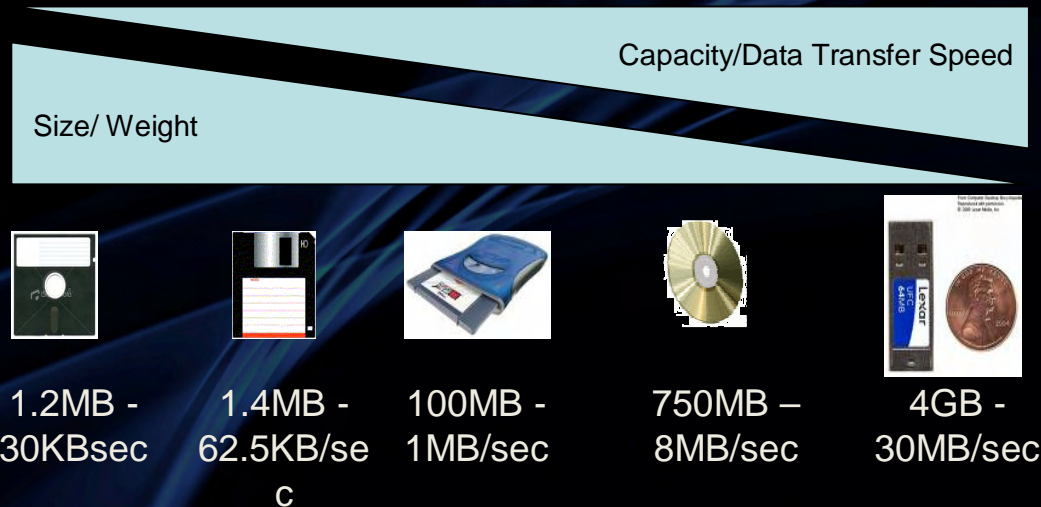
System & Network Boundaries



The problem with USB

USB Flash Drives (UFDs)

- Universally supported
- High Capacity
- High Performance
- Plug-n-play
- Microsoft Monoculture
- User Friendly
- Hacker friendly too!



C

What if I could...

- Put a custom payload on a USB stick
- Convince authorized users to connect it
- Depend on target systems to run it
- Bypass antivirus
- Bypass firewall
- Blind intrusion detection systems
- Persist over time



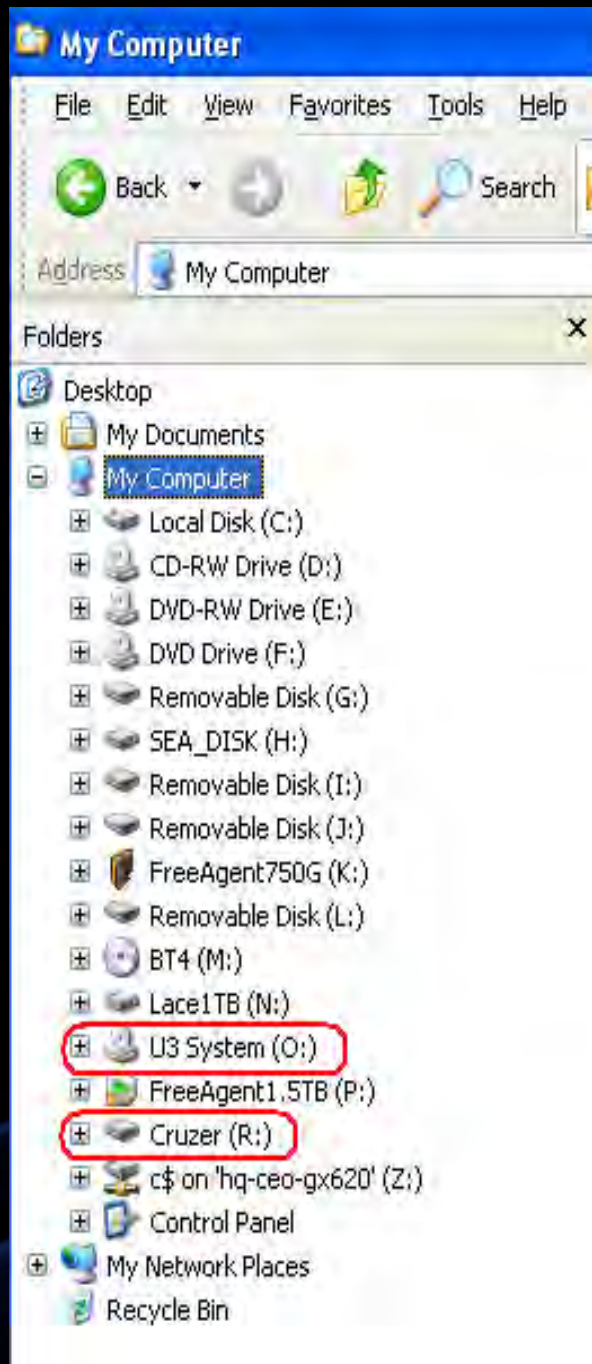
How Autorun Works

- Insert removable media
- Windows mounts it
- Autoplay will search for “autorun.inf”
- Execute “autorun.inf” if found
- Several “fixes” – registry, GPOs, etc

The U3 Challenge



- Similar to Autorun / Autoplay
- Presents itself as a CD drive and a FAT partition
- Optional password protection of FAT partition
- Entices user to click things they shouldn't
- More challenging to protect against



Building our Switchblade

Our U3 Switchblade

```
/
LaunchU3.exe
Launchpad.zip
Autorun.inf
Go.vbs
├── SYSTEM
│   ├── Logs
│   └── SRC
│       ├── HS
│       └── VNC
```

U3 boot firmware

Read-only Boot Partition

```
/
├── Logs
├── SRC
│   ├── drv.dat
│   ├── PL.dat
│   └── Include
│       ├── 0.dat
│       ├── 1.dat
│       ├── 2.dat
│       ├── .
│       ├── .
│       ├── .
│       └── ##.dat
```

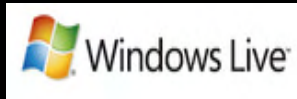
Read-write Data Partition

Passwords

Autologon passwords



Windows Local SAM







Wireless wzcfg



Dialup VPN



Browser Objects

				
Passwords	<input type="checkbox"/>			<input type="checkbox"/>
Cookies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
History	<input type="checkbox"/>	<input type="checkbox"/>		
Cache	<input type="checkbox"/>	<input type="checkbox"/>		
Favorites	<input type="checkbox"/>	<input type="checkbox"/>		
Searches	<input type="checkbox"/>	<input type="checkbox"/>		

Other G2

- User Profiles
- Last 10 user logins
- Wifi keys – wzcfg
- Product Keys – Office, Windows, Exchange, SQL
- Windows Updates
- System Services & Versions
- Network Services & Ports
- Port Scan
- Reverse Shell

Demonstration

The background of the slide is a dark, almost black, gradient. On the right side, there are several flowing, translucent blue lines that curve and overlap, creating a sense of motion and depth. The lines are most prominent in the lower right quadrant and extend towards the center.

We Just...

- Put a custom payload on a USB stick
- Convinced authorized users to connect it
- Bypass antivirus
- Bypass firewall
- Blinded intrusion detection systems
- Persisted over time

Consequences & Impacts

Or: Why you should care

Consequences & Impacts

- Significant.
- Loss of customer & corporate data;
- Loss of confidence / market share;
- Business disruption: financial impact (TJX & Heartland); law enforcement involvement
- Productivity loss
- Increased operational expense



Mitigation Strategies

People, Process and Technology

People

- Closest to the problem
- Have a job to do
- Weakest link
- Low cost / high return
- Journey not a destination



EVERYONE MUST PLAY BALL

Executives, Business Managers, Users, I.T. Staff

Process

- Policy
- Training
- Risk analysis
- Cost of Exposure or Leaks
- Value / Risk Matrix
- Tiered controls aligned with Information Risk/Value
- Not all information is created equal
- Identify Data Owners
- Taxonomize or Classify Data



Technology

- Always on
- Central management
- Policy based controls
- Directory integration
- Overrides for remote users
- No-cost, low-cost & pricey
- Pick the right tool(s) for the job
- **Safend**, Pointsec, Lumension...



Not-so-evil Switchblades

Incident Response

- Low cost
- User friendly
- FedEx ready
- Automated
- Network enabled
- Updateable as needs change



Demonstration

The background of the slide is a dark, almost black, gradient. On the right side, there are several flowing, translucent blue lines that curve and overlap, creating a sense of motion and depth. The lines are most prominent in the lower right quadrant and extend towards the center.



ISO 9001:2000 Certified

Steve Goldsby

Integrated Computer Solutions, Inc.

Steve.Goldsby@ICSInc.com

334.221.3833

www.ICSinco.com

Supplemental Slides

Risk Matrix

	Training	Desktop Hardening	AV/HIPS	Thin Client	Protective Markings	Proxy FW	SSL	SCM
Email	<		<		<	<		<
FTP	<					<		<
HTTP	<					<		<
IM	<		<			<		<
P2P	<		<			<		<
SSL Tunneling	<					<	<	
Removable Media	<		<	<				<
Classification Errors	<				<			
Hardcopy Theft	<							
Photos	<							
Malware	<		<			<		
Hacker Penetration	<		<					
Social Engineering	<							
Dumpster Diving	<							
Phishing	<					<		
Physical Theft	<			<				