

RSA[®]Conference2017

San Francisco | February 13–17 | Moscone Center

POWER OF
OPPORTUNITY

SESSION ID: MBS-W10F

The Internet of Criminal Things

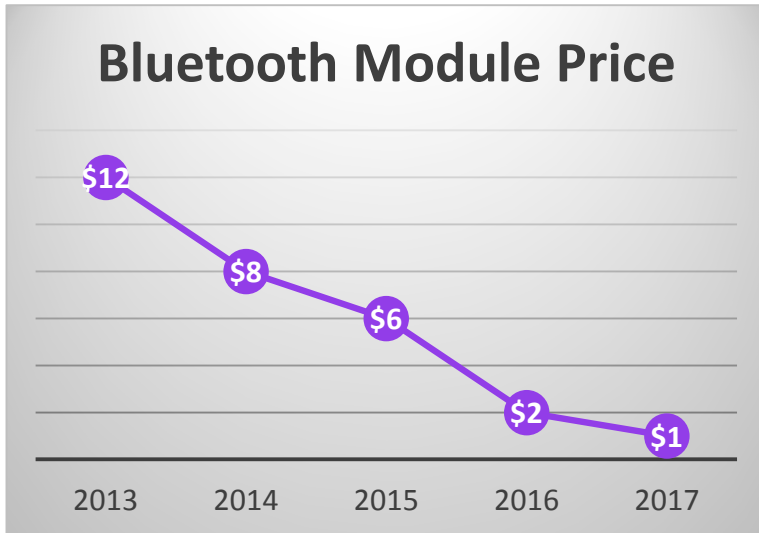


Aaron Turner

VP – Security Product Research & Development
Verifone

Understanding the Underlying Tech Market

- Just as with the 'Internet of Things', the commoditization of technology has allowed for its integration into EVERYTHING
- Bluetooth as a case study:



A screenshot of an Alibaba.com product page for a Bluetooth module. The page shows the product title, price, and supply information. The product is an HC05 HC-05 master-slave 6pin JY-MCU anti-reverse, integrated Bluetooth serial pass-through module, wireless serial. The price is listed as US \$1 - 2.5 / Piece. The supply ability is 300 Set/Sets per Week, and the port is shenzhen. There are buttons for 'Contact Supplier' and 'Start Order'.

Alibaba.com Global trade starts here™

Sourcing Solutions Services & Membership Help & Community Selector

Categories Products What are you looking for... Search

About 1 results: Wireless Networking Equipment (1)

Home > Products > Telecommunications > Communication Equipment > Wireless Networking Equipment (245770) Subscribe to Trade Alert

HC05 HC-05 master-slave 6pin JY-MCU anti-reverse, integrated Bluetooth serial pass-through module, wireless serial

FOB Reference Price: [Get Latest Price](#)

US \$1 - 2.5 / Piece | 1 Piece/Pieces (Min. Order)

Supply Ability: 300 Set/Sets per Week
Port: shenzhen

[Contact Supplier](#) [Start Order](#)

Understanding 'Skimming' Operations

- Prior to IoCT: Lots of risk - Fuel Dispenser example

Obtain master key
Understand credit card terminal layout
Block surveillance cameras
Open dispenser cabinet, install skimmer
Close cabinet, run test transaction
Open cabinet, verify transaction capture
Close cabinet, clear surveillance camera
Drive away, let sit for 2-4 days
Return to site, block surveillance camera
Open cabinet, uninstall first skimmer
Verify data capture
Install second skimmer
Close cabinet, run test transaction
Open cabinet, verify transaction capture
Close cabinet, clear surveillance camera
Drive away, let sit 2-4 days
... Repeat ...

- After IoCT: Risk Reduction!

Obtain master key
Understand credit card terminal layout
Block surveillance cameras
Open dispenser cabinet, install skimmer
Pair with mobile device, run test transaction
Close cabinet, clear surveillance camera
Drive away, let sit for 2-4 days
Return to within Bluetooth range, dump transaction data
Drive away, let sit for 2-4 days
... Repeat ...

Average install time for experienced operators reduced from ~15 minutes to ~30 seconds

Most operators apprehended upon physical retrieval, IoCT significantly reduces that risk

Understanding the 'Skimming' Market

- In the US*:
 - \$4,000,000,000 annually
 - ~\$11,000,000 per day
- In Los Angeles County in 2015*:
 - A small criminal organization made \$40,000,000 from skimming



* Data courtesy US Secret Service

\$50,000
The average loss from skimming crime²



Skimming-related counterfeit card fraud is the leading type of third-party card fraud³

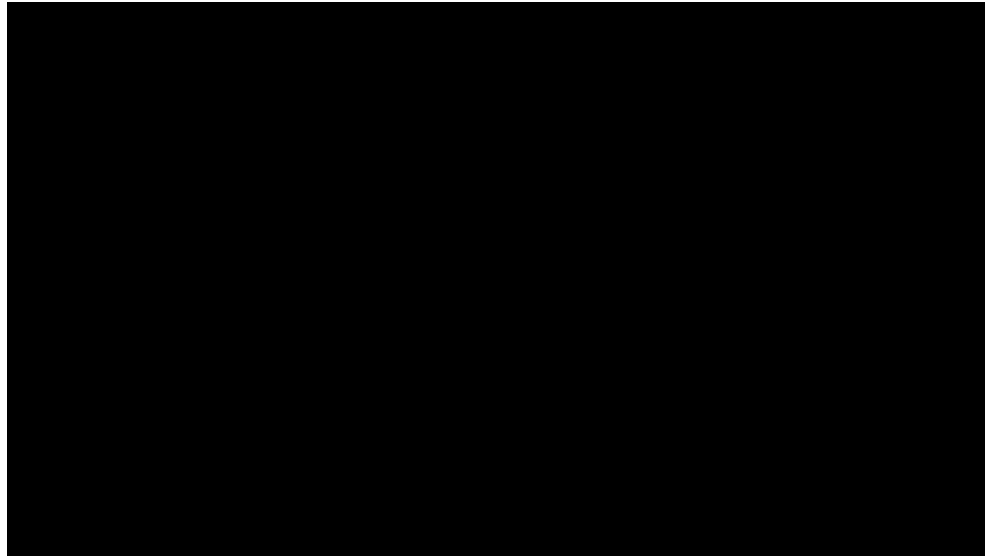


Skimming is the #1 ATM crime globally making up 92% of all attacks at the ATM¹

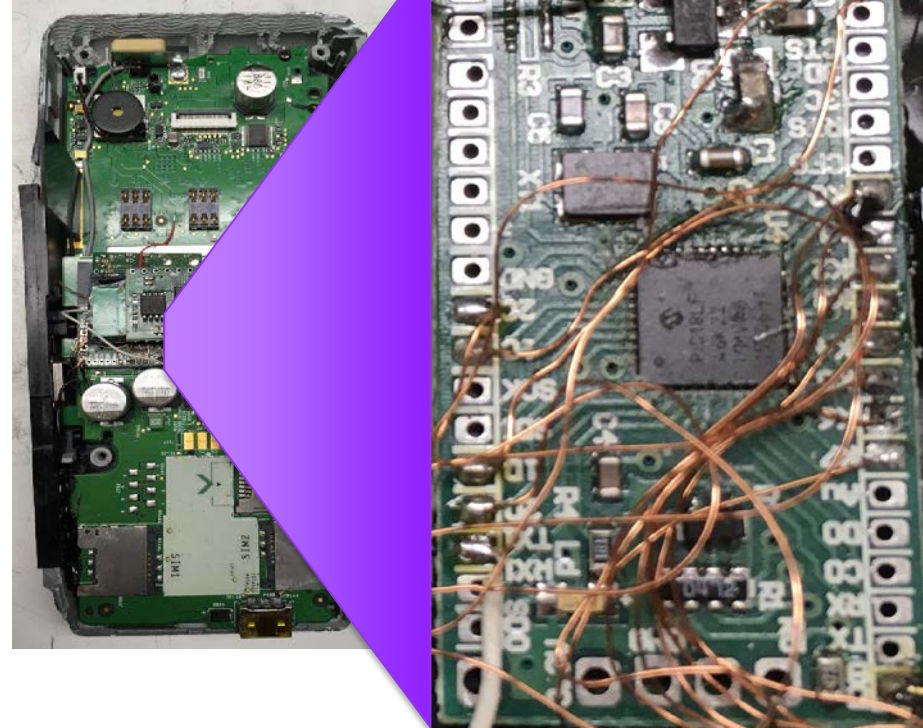
Source: PCI Security Standards Council 2015

Retail Skimmer Install

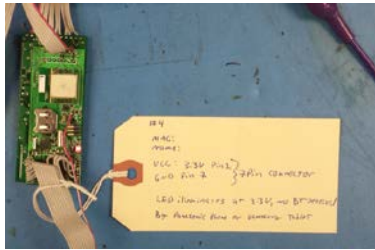
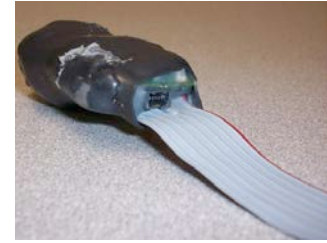
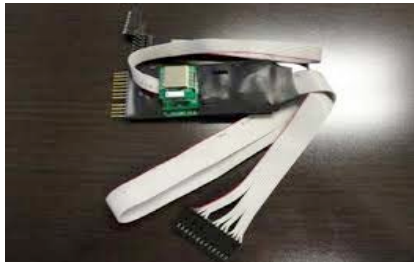
- 3D-printers + cheap integrated circuits = profit!



Innovation!

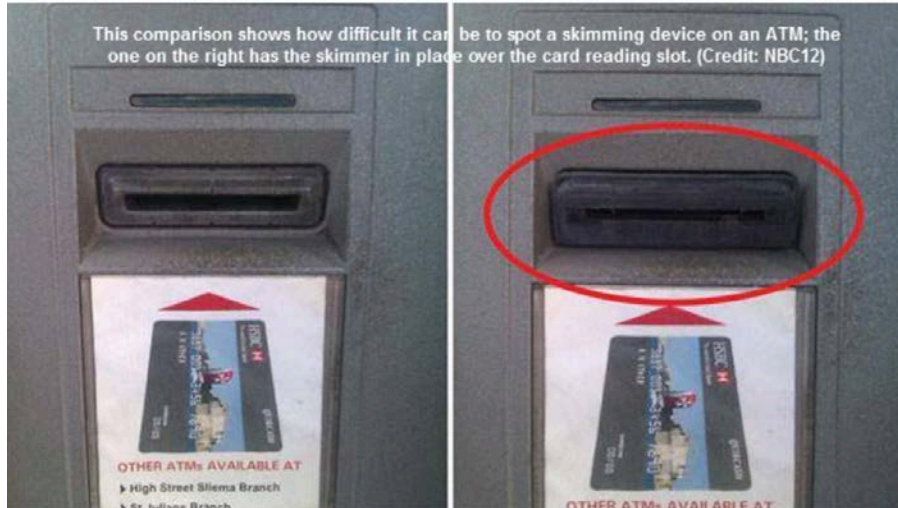


All shapes and sizes...



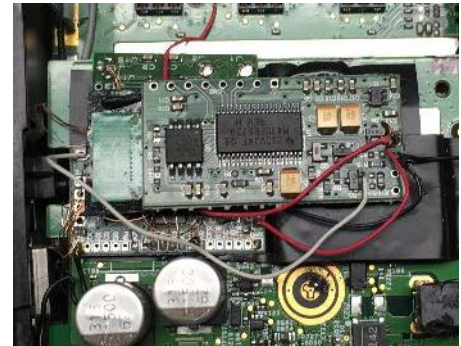
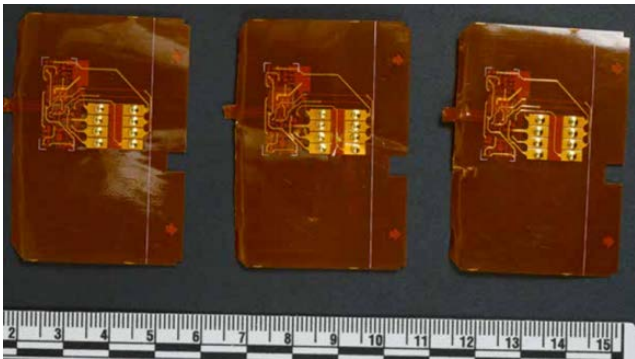
ATM Skimmer Market

- ATM skimming spiked 546% in 2015
- Bank & non-bank ATMs are targeted
- Nonbank ATM attacks becoming more prevalent



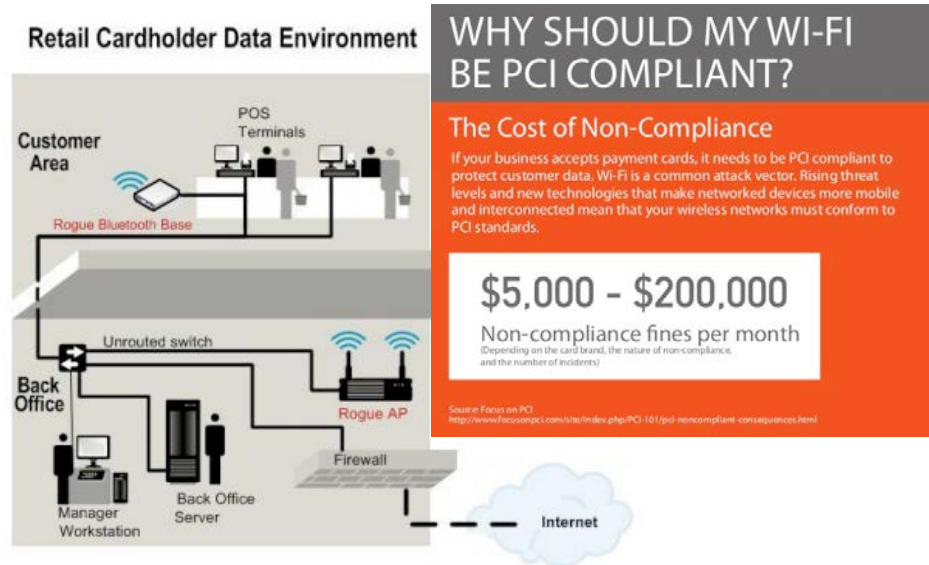
EMV Helps... sometimes

- EMV or 'chip' payment cards do prevent some types of skimming
- Skimming and shimming are both still possible due to weaknesses in some EMV deployments around the world
 - Several developing markets have ATM systems which do not do a full EMV validation on card data
 - There are static data components that can be re-used



Malicious WiFi Hotspot Problems

- PCI mandates quarterly audits & non-compliance fines possible
- Brand damage & consumer protection
- Rogue Access Point (Wi-Fi) that appear with business name and used to steal customers identity
- Unmanaged access points create potential breach entry points & potential remote access to the entire network



Commoditized IoCT Market



Sourcing Solutions ▾

Services & Membership ▾

Help & Community ▾

☰ Categories ▾

Products ▾

atm skimmers for sale

Related Searches for atm skimmers for sale: used atm machines for sale complete atms b

☰ Related Category

Home > Service Equipment > atm > atm skimmers for sale < 1,328 Results

ICQ: 612384658



MSR Tron - MSR-Basic Interrupted Swipe Card...



ATM Skimmers Available Direct From Middle East...



ATM Skimmers for Sale Full Kit Ncr , Wincor



atm skimmer diebold msrtron



ATM SKIMMER FOR SALE INSERT MODEL SKIMME...



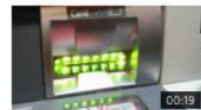
ATM SKIMMER FOR SALE USA MODEL 2016



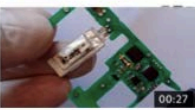
MSR Tron - DB001 ATM Bezel Overlay



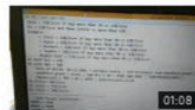
MSR Tron - NR001 ATM Bezel Overlay



Diebold ATM Skimmer Review



ATM SKIMMER FOR SALE INSERT MODEL SKIMMER DEVICE



Sell cc , ccv fullz info(ICQ:690729420;Yah...



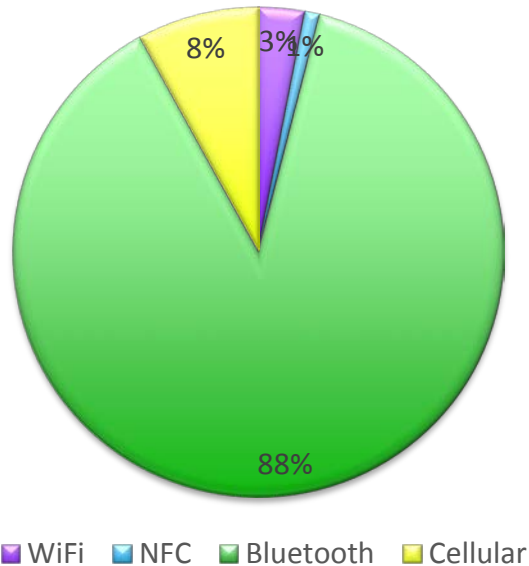
ATM SKIMMER FOR SALE 2016 USA MODELS FACTORY PRICE

Solutions Gap

- What is the commonality among IoCT devices? WIRELESS
- How can organizations scalably detect IoCT devices? Wireless Sensors
- But...
 - The current wireless sensor market does not address the real-world problem
 - US and EU regulations do not provide clear guidance on the legality of deploying wide-spectrum wireless sensors
 - Communications Act of 1933 did not contemplate IoCT – SHOCKING!

Skimmer Wireless Technology Deployment

Skimmer Wireless



- Bluetooth skimmers represent by far the largest deployment of wireless IoT technologies
- Cellular is rapidly growing with the drop in LTE modem module pricing



Unlocked Wireless DW5804
PCI-E 3G/4G Card WLAN WC
★★★★★ 5.0 (1 votes) | 2 or

Price: US \$19.50 / piece
Discount Price: **US \$18.53** /

Shipping: **Free Shipping to Un**
Estimated Delivery Ti

Quantity: + p

Total Price: **US \$18.53**

Buy Now Ad

Technical Challenges to IoCT Detection

- WiFi:
 - Most 'smart' devices no longer broadcast their MAC address unless actively associated with a Wireless Access Point
- Bluetooth:
 - Once paired, MAC addresses are obfuscated by white noise and not detectable until they go back into 'discoverable' mode
- NFC:
 - High-gain antennas required for most detection and monitoring (3-6 feet in size)
- Cellular:
 - Distributed antenna systems required for site-wide monitoring, very high costs

Critical breakthroughs in IoCT detection

- Bluetooth - Moore's law is helping us

- Consortium of researchers have developed 'BlueBrute'
- Low-cost Bluetooth white-noise stripper
- Current prototype can leverage FPGA's

Pkts	Time (ns)	Channel	Access Address	Adv PDU Type	Adv PDU Header	AdvA	AdvData	CRC (dBm)	RSSI (dBm)	FCS
1	+0	0x26	0x00000000	ADV_IND	Type: Tab0d Tab0d PDU-Length: 0 33	0x00110040C2B3	02 01 04 11 04 BA 56 59 A4 FA BF A2 80 01 44 78 4E 73 34 AB 20 33 14 0A 18 07 04	0x005E5A3D	-44	OK
2	+1299367 +1299504	0x26	0x00000000	ADV_IND	Type: Tab0d Tab0d PDU-Length: 0 33	0x00110040C2B3	02 01 04 11 04 BA 56 59 A4 FA BF A2 80 01 44 78 4E 73 34 AB 20 33 14 0A 18 07 04	0x005E5A3D	-44	OK
3	+9448 +1393835	0x26	0x00000000	ADV_IND	Type: Tab0d Tab0d PDU-Length: 0 33	0x00110040C2B3	02 01 04 11 04 BA 56 59 A4 FA BF A2 80 01 44 78 4E 73 34 AB 20 33 14 0A 18 07 04	0x005E5A3D	-44	OK
4	+201146 +2895503	0x26	0x00000000	ADV_IND	Type: Tab0d Tab0d PDU-Length: 0 33	0x00110040C2B3	02 01 04 11 04 BA 56 59 A4 FA BF A2 80 01 44 78 4E 73 34 AB 20 33 14 0A 18 07 04	0x005E5A3D	-44	OK
5	+1302499 +3897502	0x26	0x00000000	ADV_IND	Type: Tab0d Tab0d PDU-Length: 0 33	0x00110040C2B3	02 01 04 11 04 BA 56 59 A4 FA BF A2 80 01 44 78 4E 73 34 AB 20 33 14 0A 18 07 04	0x005E5A3D	-44	OK
6	+4728428 +46497	0x26	0x00000000	ADV_IND	Type: Tab0d Tab0d PDU-Length: 0 33	0x00110040C2B3	02 01 04 11 04 BA 56 59 A4 FA BF A2 80 01 44 78 4E 73 34 AB 20 33 14 0A 18 07 04	0x005E5A3D	-44	OK
7	+5384979	0x26	0x00000000	ADV_IND	Type: Tab0d Tab0d PDU-Length: 0 33	0x00110040C2B3	02 01 04 11 04 BA 56 59 A4 FA BF A2 80 01 44 78 4E 73 34 AB 20 33 14 0A 18 07 04	0x005E5A3D	-44	OK

- Cellular – DAS commoditization

- Working with new base station partners to deploy 3-sensor cellular arrays to detect persistent cellular signals locations based on square-centimeter fidelity
- Still years away from field deployments, but a path forward as cellular IoCT deployment increases

Policy and Legal Clarity?

- At present is it legal for organizations to...
 - Persistently monitor for the presence of IoT devices?
 - It depends... wait... we're not sure... umm...
- Pushing for clarity with FCC, Center for Democracy and Technology, Congress and others
 - Proposed legislation to carve out specific rights for property owners to monitor addressing and signaling information (not content) for unauthorized devices which may pose a risk to their guest's personal information

Near-term Action Plans

- Deploy persistent RF sensing arrays with back-end analysis tools
- Verifone has partnered with Pwnie Express to do significant research into this space.
 - Discovered skimmers in addition to malicious access points and drones with WiFi attack gear attached to them
 - Pwnie's Pulse Platform has real potential in this area
- Understand what 'normal' RF signal spectrum should look like ASAP to then establish processes for detecting 'anomalies'
- Demand better solutions from the current spectrum monitoring providers