Cybersecurity research: Stories from the trenches

Stefan Savage
UC San Diego

What do we mean when we say "security"?

What do we mean when we say "security"?

- Merriam-Webster online dictionary:

Function: *noun*

1 : the quality or state of being secure : as a : *freedom from danger* : SAFETY b *: freedom from fear or anxiety* c : freedom from the prospect of being laid off <job security>

k

4 a : something that secures : PROTECTION b (1) : measures taken to guard against espionage or sabotage, crime, attack, or escape (2) : an organization or department whose task is security

Freedom from danger

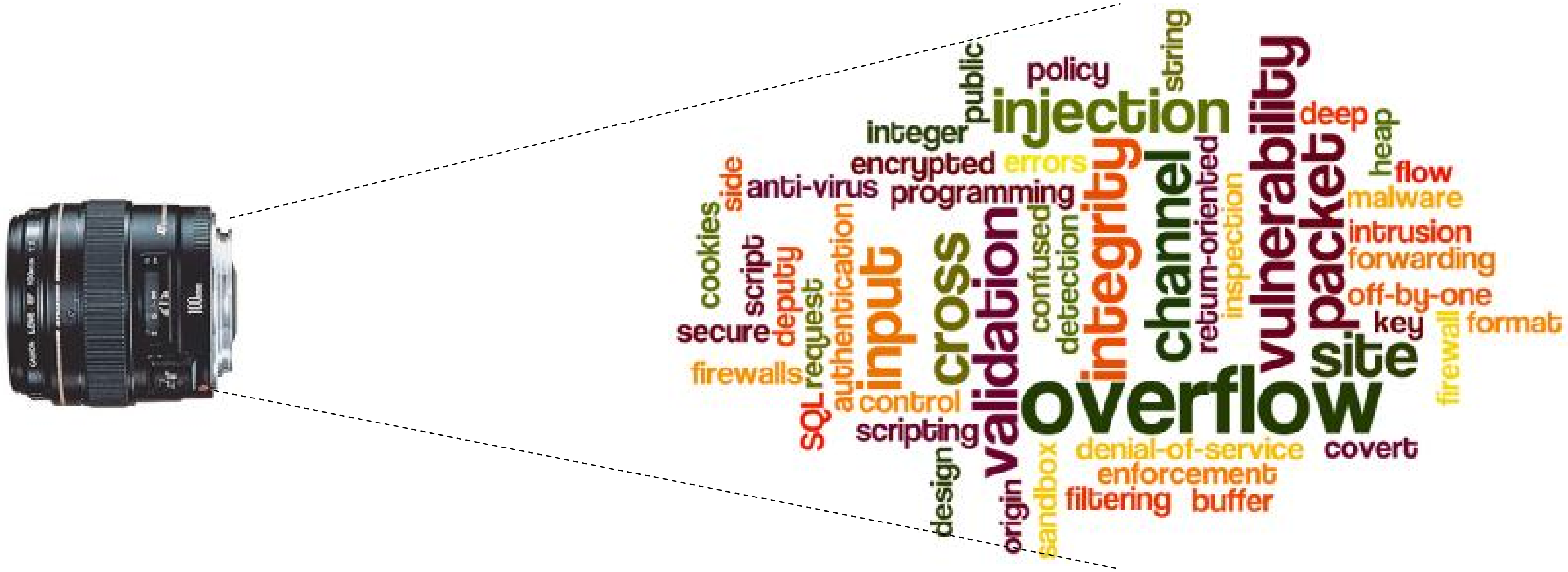
Freedom from fear or anxiety

Fears and dangers are driven by technological change

Fears and dangers are driven by technological change

What is the security problem?

- Cybersecurity is a technical problem



- Yes, but only part of the puzzle; solving technical problems does not stop attackers

UCSDCSE
Computer Science and Engineering

What is the security problem?

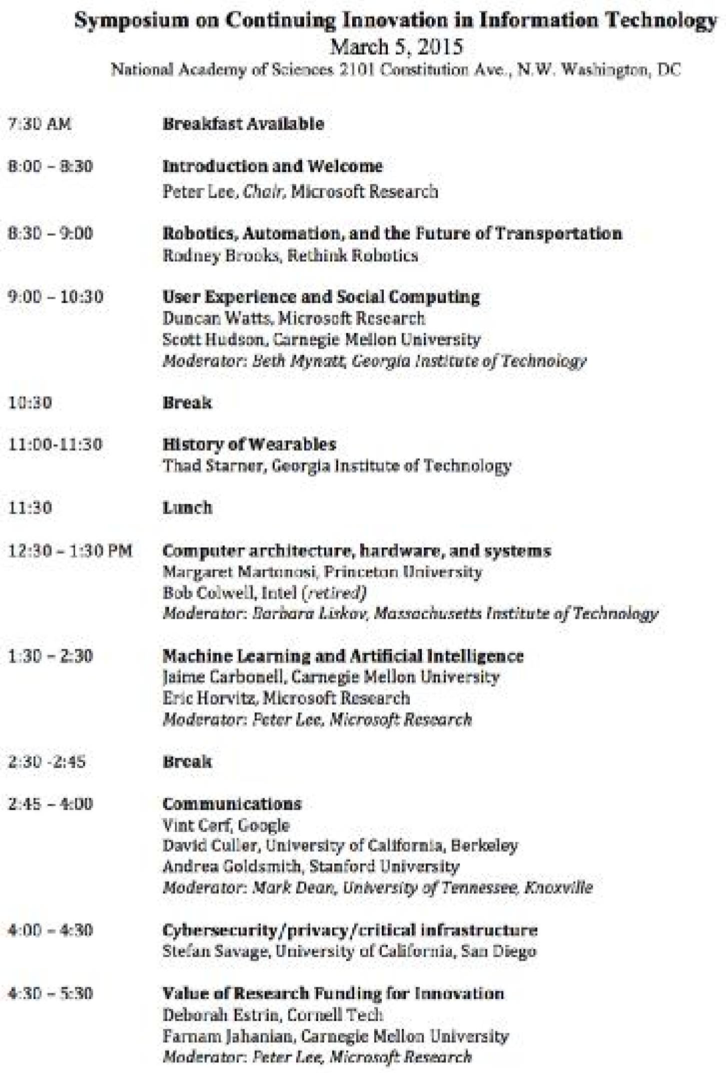
- Cybersecurity is a socio-economic problem

  - Actors
    - Adversaries
    - Victims
    - Defenders
  - Incentives/Costs
  - Relationships
- Yes, but technology defines the “medium” of the conflict

Cybersecurity is *fundamentally* a cross-cutting discipline

How do we provide all this functionality…

while in the presence of an adversary?



Symposium on Continuing Innovation in Information Technology
March 5, 2015
National Academy of Sciences 2101 Constitution Ave., N.W. Washington, DC

7:30 AM	**Breakfast Available**
8:00 – 8:30	**Introduction and Welcome** Peter Lee, *Chair*, Microsoft Research
8:30 – 9:00	**Robotics, Automation, and the Future of Transportation** Rodney Brooks, Rethink Robotics
9:00 – 10:30	**User Experience and Social Computing** Duncan Watts, Microsoft Research Scott Hudson, Carnegie Mellon University *Moderator: Beth Mynatt, Georgia Institute of Technology*
10:30	**Break**
11:00-11:30	**History of Wearables** Thad Starner, Georgia Institute of Technology
11:30	**Lunch**
12:30 – 1:30 PM	**Computer architecture, hardware, and systems** Margaret Martonosi, Princeton University Bob Colwell, Intel *(retired)* *Moderator: Barbara Liskov, Massachusetts Institute of Technology*
1:30 – 2:30	**Machine Learning and Artificial Intelligence** Jaime Carbonell, Carnegie Mellon University Eric Horvitz, Microsoft Research *Moderator: Peter Lee, Microsoft Research*
2:30 -2:45	**Break**
2:45 – 4:00	**Communications** Vint Cerf, Google David Culler, University of California, Berkeley Andrea Goldsmith, Stanford University *Moderator: Mark Dean, University of Tennessee, Knoxville*
4:00 – 4:30	**Cybersecurity/privacy/critical infrastructure** Stefan Savage, University of California, San Diego
4:30 – 5:30	**Value of Research Funding for Innovation** Deborah Estrin, Cornell Tech Farnam Jahanian, Carnegie Mellon University *Moderator: Peter Lee, Microsoft Research*

UCSDCSE
Computer Science and Engineering

30 years of research underlies most of today's cybersecurity technology

- Vulnerability finding tools, safe languages
- Anti-malware, TPMs
- Exploit mitigation (ASLR, DEP, SFI/CFI)
- Virtual machine isolation
- Virtual private networks, SSL/TLS
- Network defenses
  - Firewalls, intrusion detection, data leakage protection
- Two-factor authentication

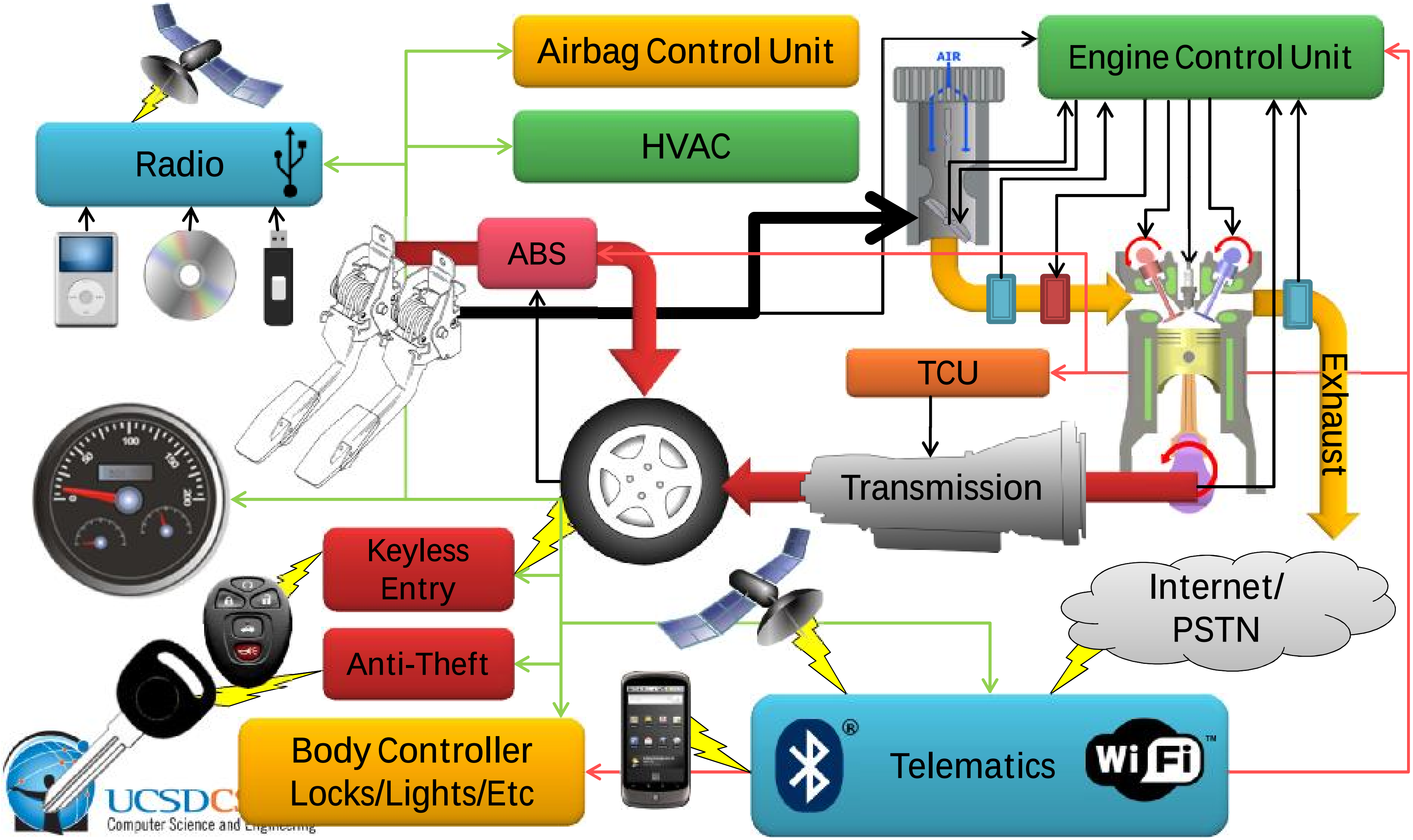
But equally important in supporting key public policy questions

- Two quick research stories focused on
  - Transportation: identifying and understanding nature of cyber risks in modern automobiles (creating institutional focus around risk)
  - Intellectual property: how to best tackle abusive advertising of counterfeit goods? (quantifying effective ways to address threat)

Transportation is computerized

One example is automobiles

The modern automobile...



Bottom line:
Cars are heavily computerized

- Today's car is a big distributed system
  - Complex computerized control
    - Millions of lines of code
    - Many 10s of distinct computers (ECUs)
  - Shared internal networking (e.g., CAN, FlexRay)
  - Increasing external communications features
    - Telematics, Bluetooth, TPMS, RDS, XM radio, GPS, keyless start/entry, USB ports, WiFi, etc
- Tomorrow's car -> much more of everything
  - V2V/ACAS, V2I, traffic control, autonomous driving

What we did

- We (UCSD/UW) bought some automobiles
  - Reverse engineered aspects of networks and ECUs
  - Actively tested robustness to adversarial input
  - Detailed results at autosec.org

- Two phases
  - Analyze the resilience of internal systems
    - i.e., how bad is it if the radio gets compromised?
  - Analyze external attack surface
    - i.e., can you compromise a vehicle without physical access?

Security punchline

One can obtain arbitrary control of a vehicle at arbitrary distance with no prior physical access

Validated attack vectors

- Auto service tools
  - WiFi to OBD-II bridge; Internet accessible
  - Bug in tool; takes over all cars that visit dealership

- CD Player
  - Bug in media parsing option; also legacy update code
  - Song that, when played, takes over player

- Bluetooth via phone-based malware
  - Paired phone can trigger vuln (also possible to brute force)
  - Malicious app can take over car

- Telematics
  - Remote exploit via audio in-band control channel
  - Can call the car and take it over by playing in-band audio signal

Example: Involuntary Braking

Why so many problems?

- Biggest reason: Lack of adversarial pressure
  - No one is attacking computers in cars today
  - Consequently, only modest investment (until recently) in security measures
  - Common to almost all of "Internet of Things" today

- Manifestations
  - Existing security not designed for strong adversaries
  - No std fuzz testing, security analysis tools, etc
  - Code rife with "old" vulnerabilities, e.g., strcpy
  - "Standard" mitigations don't exist (e.g. ASLR, DEP)
  - Roll-your-own authentication protocols
  - Attacker-friendly environments (e.g. symbols, interactive shells and tools)

UCSDCSE
Computer Science and Engineering

Extra-technical challenges

- Large and growing external attack surface
  - Telematics, V2I, V2V, autonomous driving, in-car Wifi, Smart phone integration, 3rd-party modules
  - Fundamentally complex system; can’t isolate physically
- Complex supply chain
  - Collection of integrated computer systems
  - Top-to-bottom security review near impossible; e.g., no single party has the source code
- Structural economic challenges
  - Low margin cost structures
  - Manufacturers can’t compete on security
- No efficient update mechanism

What happened?

- Short term
  - Worked to fix software for 10+M vehicles
  - Mitigations w/carriers & manufacturers
- Medium term
  - Manufacturers: investment (10x increase in staffing)
    - Significant changes in software processes
    - OTA update, security incident response
  - Standards: New cyber standards in SAE
  - Regulatory: NHTSA takes ownership of cyber
- Longer term
  - Cyberphysical security research programs (HACMS, CPS)

Switching gears…

We spend lots of money on security

- We are constantly trying to keep up

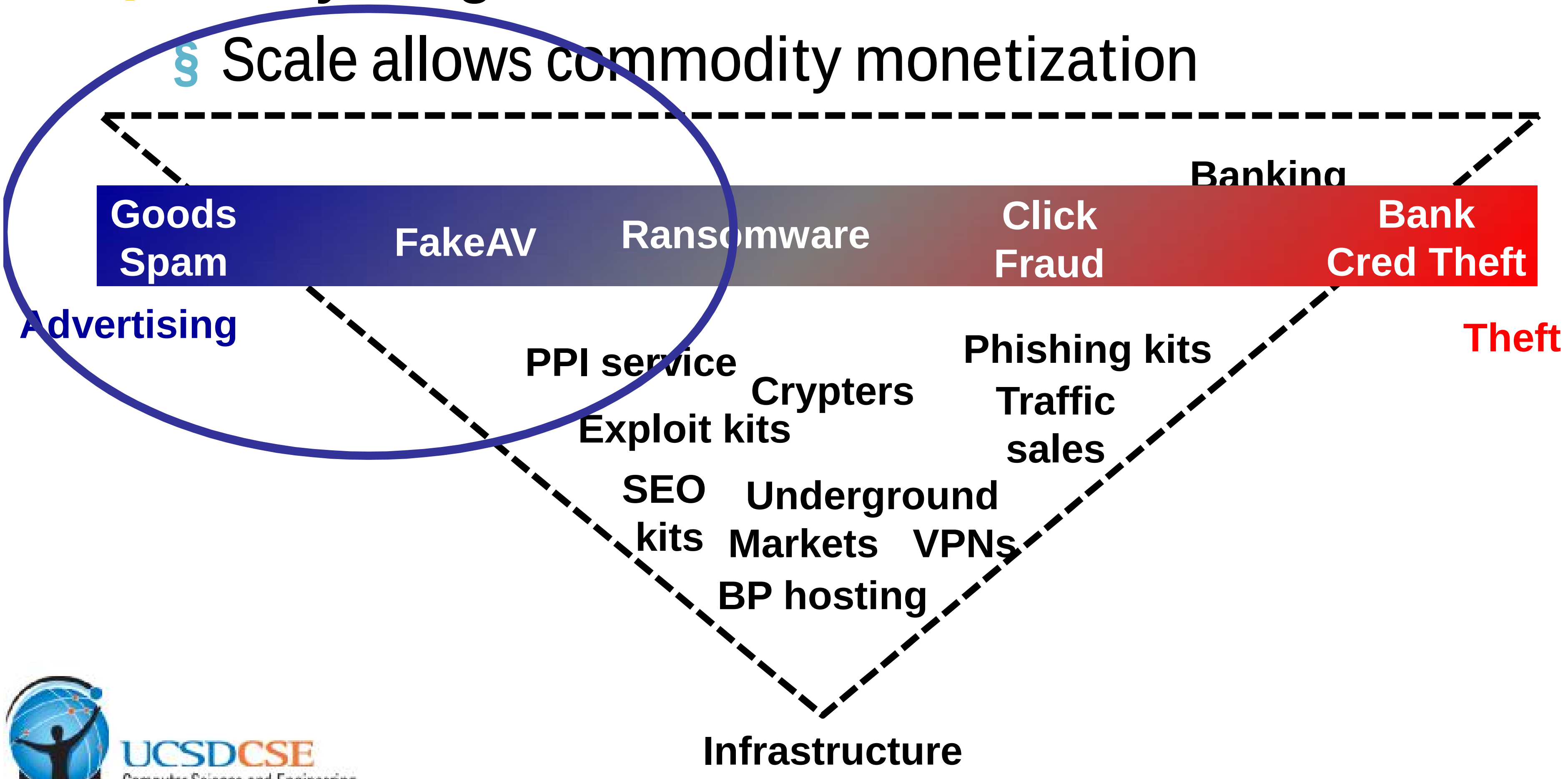
- How should we reason about the security investments we make?

Challenge: structural asymmetries

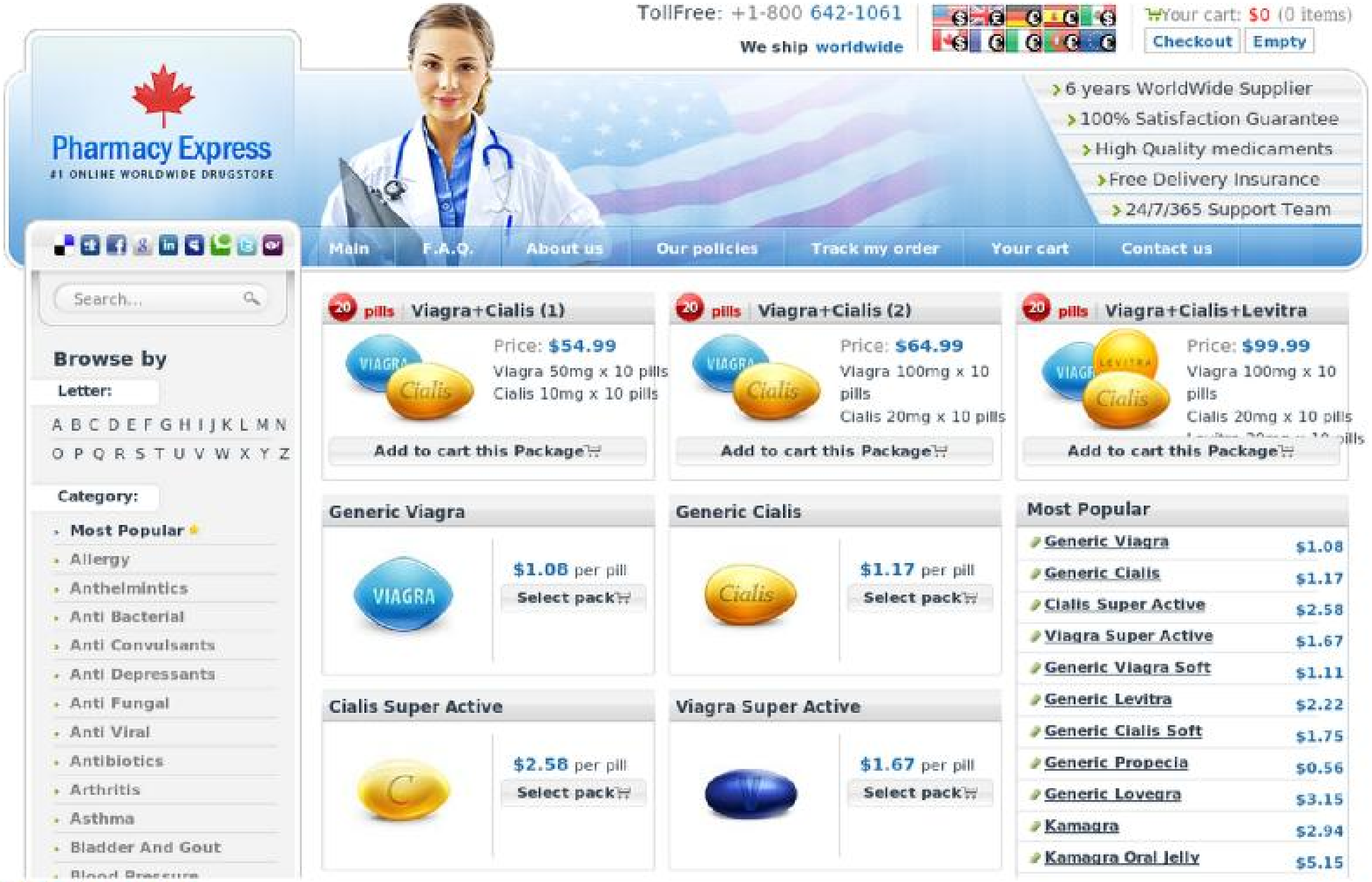
- Attacks easy to measure, defenses hard
  - Attackers can usually measure success/ROI
    - Well-defined cost structures (e.g., 1k machines=~$100, 1k accts = ~$8)
    - Frequently well-understood business processes (advertising, theft, extortion)
  - Defensive security metrics largely non-existent
    - Process oriented (e.g., coverage tests)
- Key thought: use attacker metrics to evaluate interventions

Economics of online abuse

- Today, largest driver for online threats is $$$
  - Scale allows commodity monetization



A banal example of the problem



TollFree: +1-800 642-1061

We ship worldwide

Your cart: $0 (0 items)

Checkout | Empty

Pharmacy Express

#1 ONLINE WORLDWIDE DRUGSTORE

- 6 years WorldWide Supplier
- 100% Satisfaction Guarantee
- High Quality medicaments
- Free Delivery Insurance
- 24/7/365 Support Team

Browse by

Letter:

A B C D E F G H I J K L M N
O P Q R S T U V W X Y Z

Category:

- Most Popular
- Allergy
- Anthelmintics
- Anti Bacterial
- Anti Convulsants
- Anti Depressants
- Anti Fungal
- Anti Viral
- Antibiotics
- Arthritis
- Asthma
- Bladder And Gout
- Blood Pressure

20 pills Viagra+Cialis (1)

Price: $54.99
Viagra 50mg x 10 pills
Cialis 10mg x 10 pills

Add to cart this Package

20 pills Viagra+Cialis (2)

Price: $64.99
Viagra 100mg x 10 pills
Cialis 20mg x 10 pills

Add to cart this Package

20 pills Viagra+Cialis+Levitra

Price: $99.99
Viagra 100mg x 10 pills
Cialis 20mg x 10 pills
Levitra 20mg x 10 pills

Add to cart this Package

Generic Viagra

$1.08 per pill
Select pack

Generic Cialis

$1.17 per pill
Select pack

Cialis Super Active

$2.58 per pill
Select pack

Viagra Super Active

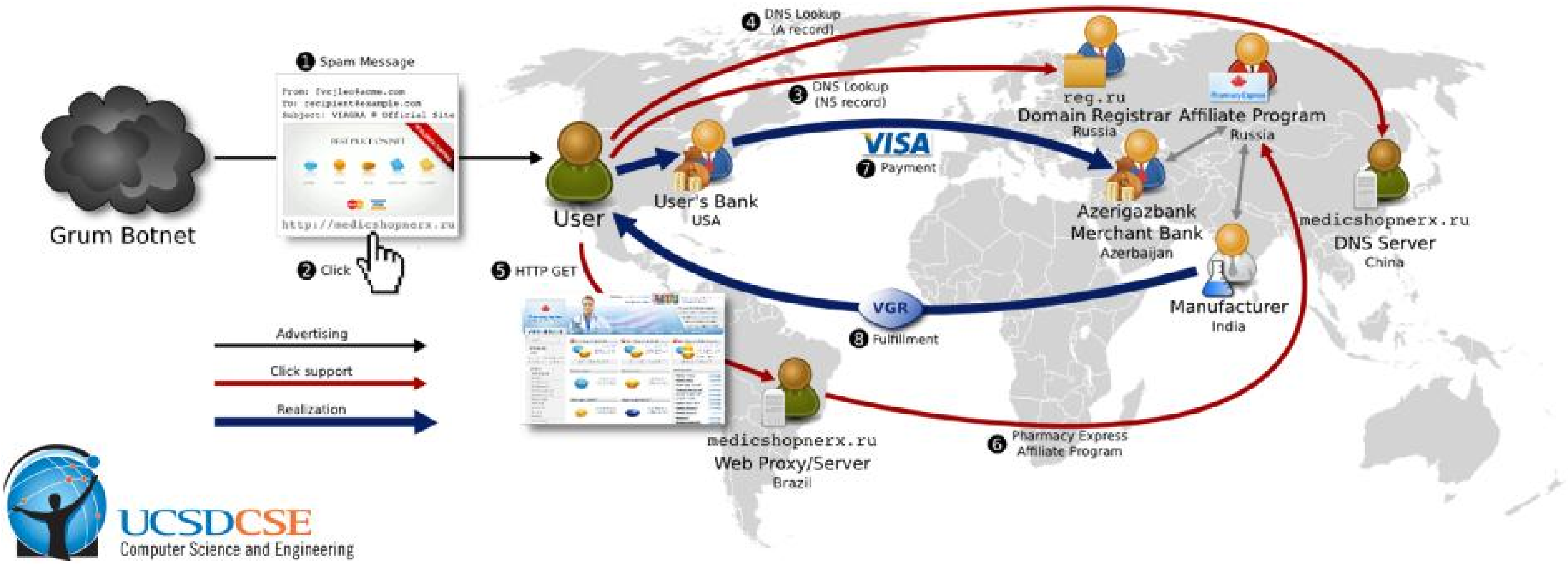
$1.67 per pill
Select pack

Most Popular

Generic Viagra	$1.08
Generic Cialis	$1.17
Cialis Super Active	$2.58
Viagra Super Active	$1.67
Generic Viagra Soft	$1.11
Generic Levitra	$2.22
Generic Cialis Soft	$1.75
Generic Propecia	$0.56
Generic Lovegra	$3.15
Kamagra	$2.94
Kamagra Oral Jelly	$5.15

Many pieces to make this work...

- E-mail spam, Web spam, OSN abuse, etc.
- Complex value chain relationships



So what to do?

- Filter spam e-mails ($1B+/yr)

- Blacklist advertised domains
- Legal avenues (DMCA, TROs)
  - Seize/takedown advertised domains
  - Remove from Search Engine results

CHANEL, INC. v. CHANEL-BESTSELL.COM, et al.

[illegible]

[illegible]

[illegible]

[illegible]

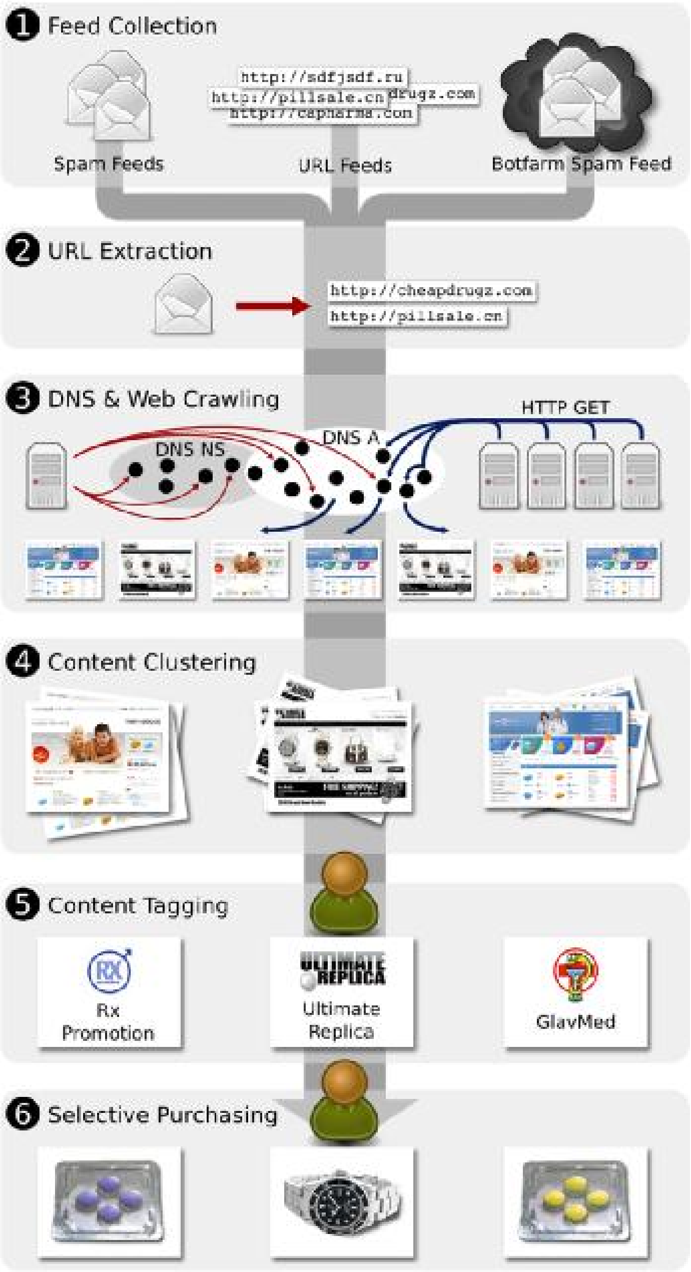
UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CASE NO.

CHANEL, INC.,

Plaintiff,

vs.

- Target payment processing

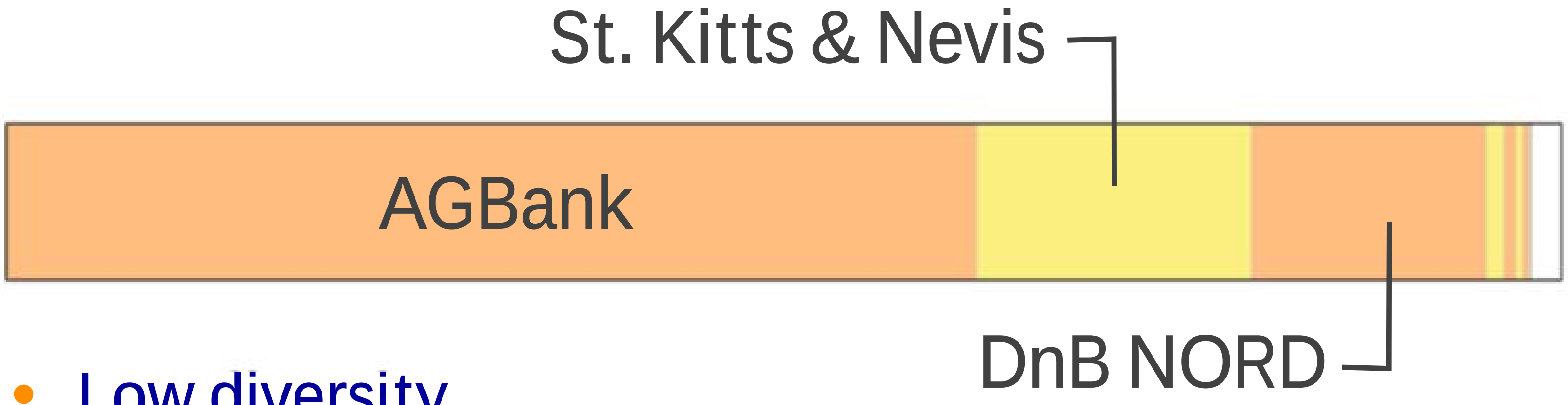


- Click Trajectories study [Levchenko, IEEE S&P 2011]
- Goal: identify key bottlenecks in spam value chain
  - Maximize switching cost
- 7 URL/Spam feeds + 5 botnet feeds
  - 968M URLs, 17M domains
  - 99% of pharma, OEM, replica
- Crawled domains for 98% of URLs
- Hundreds of purchases
  - Unique card # per order
  - Identify banks receiving $

600+ orders later…

UCSDCSE
Computer Science and Engineering

Merchant banks (circa late ‘10)



- Low diversity
  - 3 banks covered 95% of pharma/replica/software spam
  - Fewer banks willing handle “high-risk” merchants
- High switching cost
  - Time: In-person account creation, due diligence
  - Money: Upfront capital, holdback forfeiture

From research to practice

- Complex interplay of:
  - Encouragement from EOP
  - Brand interest
  - Card association cooperation
  - Complex politics around SOPA/PIPA/etc
- Leads to two major changes
  - Visa Global Brand Protection Program (GBPP)
  - Targeted merchant intervention (IACC & brands)

Office of Management and Budget

Office of the U.S. Intellectual Property Enforcement Coordinator

The New York Times

The Opinion Pages

EDITORIAL

Spammers and Their Bankers

In early 2004 Bill Gates claimed that "two years from now, spam will be solved." Today it amounts to 70 percent of all e-mail. Yet there may be a chance to cut it back.

IACC

IACC FEATURED ON CNN – MY COUNTERFEITING STING

HOW TO SPOT A FAKE

UCSDCSE
Computer Science and Engineering

Result: targeted payment intervention efforts today

- Undercover test purchase at counterfeit site
  - Get merchant bank from transaction data
- IP holder notifies card assoc (e.g., Visa/MC)
  - Investigation; complaint delivered to bank
- Leverage via card association contract
  - Merchant bank owns liability
  - Fines, increased scrutiny, de-association
- Merchant account shutdown

Example: OEM (pirate) software

cdrbsoftware
Affordable Software Titles

По вопросам регистрации и суппорта обращайтесь смело 371-377

приватная OEM-партнёрка – СИЛА!
БОЛЬШОЙ ВЫХЛОП!

OEMCash

SOFT MONSTER

WAREZSTORE.COM

software sellers

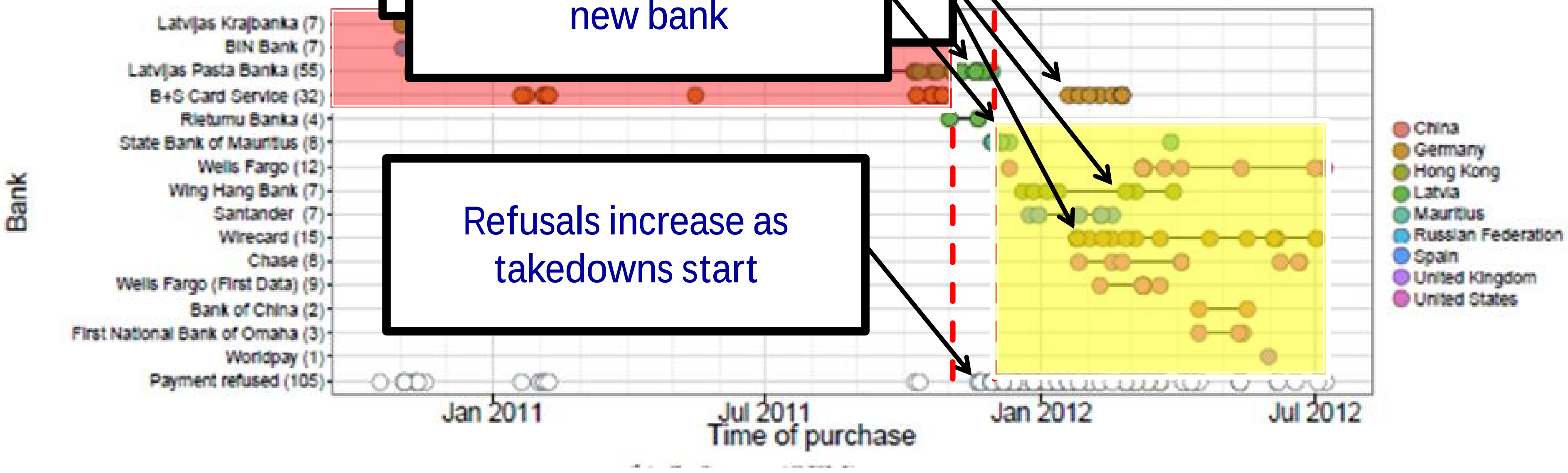
OEM Soft Store
Easy and Fast Download

OEM 2012

OEM software story

- Microsoft Thanksgiving surprise (Nov ‘11)
  - Methodically issued complaints for accounts of *every* major pirate affiliate program
  - Diligent follow up: new pr aints (and quickly)

Scramble to find stable new bank



Refusals increase as takedowns start

Qualitative Timeline

11/2011: Microsoft starts merchant complaint actions

11/20/2011: ATTENTION Dear advertisers, we are having problems with the bank and our accounts were suddenly frozen. We're forced to temporarily stop accepting OEM traffic.

ВНИМАНИЕ! Уважаемые адверты, у нас появились внезапные проблемы с банком и нам заморозили счета. Мы вынуждены временно приостановить приём OEM трафика.

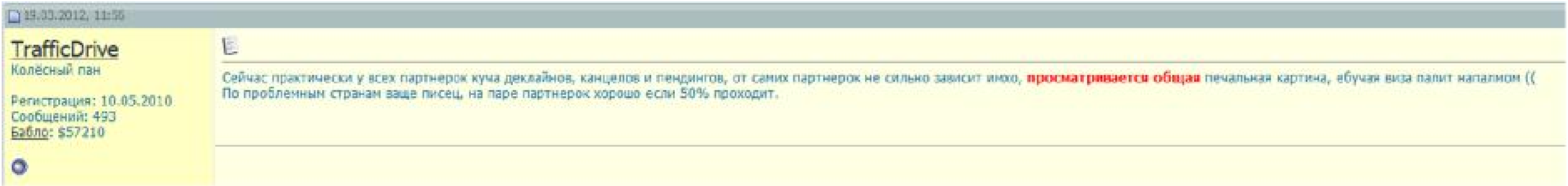
2011-11-22 10:16:38: Starting today our bank has stopped working. Due to this, we have made the decision to close our affiliate program for the duration of our search for new processing.

С сегодняшнего дня работа нашего банка приостановлена (подробнее). В связи с этим принято решение о закрытии нашей ПП на время поиска нового процессинга.

1/23/2012 Remark by leading affiliate:
"The sun is setting on the OEM era"

McCoy, Kreibich, Voelker and Savage, *Priceless: the role of Payments in Abuse-advertised Goods,*, CCS 2012.

Life is tough all around…



15.03.2012, 11:56

TrafficDrive
Колёсный пан

Регистрация: 10.05.2010
Сообщений: 493
Бабло: $57210

Сейчас практически у всех партнерок куча деклайнов, канцелов и пендингов, от самих партнерок не сильно зависит имхо, **просматривается общая** печальная картина, ебучая виза палит напалмом ((
По проблемным странам ваще писец, на паре партнерок хорошо если 50% проходит.

“Right now most affiliate programs have a mass of declines, cancels and pendings, and it doesn't depend much on the program imho, there is a general sad picture, fucking Visa is burning us with napalm (for problematic countries, it's totally fucked, on a couple of programs you're lucky if you get 50% through).”

UCSDCSE
Computer Science and Engineering

Initial Results

- As of mid-2012
  - OEM software market was decimated
  - 90% of programs have folded
  - New startups (softbuy) shut down quickly
- Hugely successful: lasted almost 24mos

- Now in effective use in a range of verticals
  - Pharmaceuticals, luxury brands, etc

Overall observations

- Security research spans incredible range
  - Every subfield, every time frame, intersects with virtually every industry, govt function
- Academia plays key role in addressing problems private sector can’t/won’t
  - Not driven by current crises; before value clear
  - Independent assessment; no one’s job
- Unusually low friction on tech transfer
  - Pain is huge catalyst for adoption

UCSDCSE
Computer Science and Engineering