Hacking the Cloud

Eugene Schultz, Ph.D., CISSP, CISM, GSLC
Chief Technology Officer
Emagined Security
EugeneSchultz@emagined.com

ISSA-LA Security Summit
West Los Angeles, California
June 15, 2011

Outline

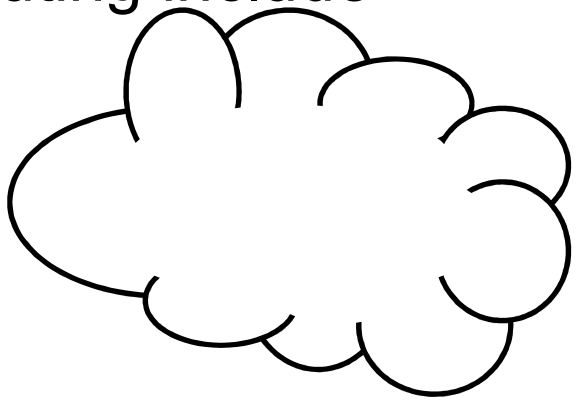
EMAGINED SECURITY

- Introduction
- Major cloud security risks
- Hacking the cloud
- Conclusion

About cloud computing

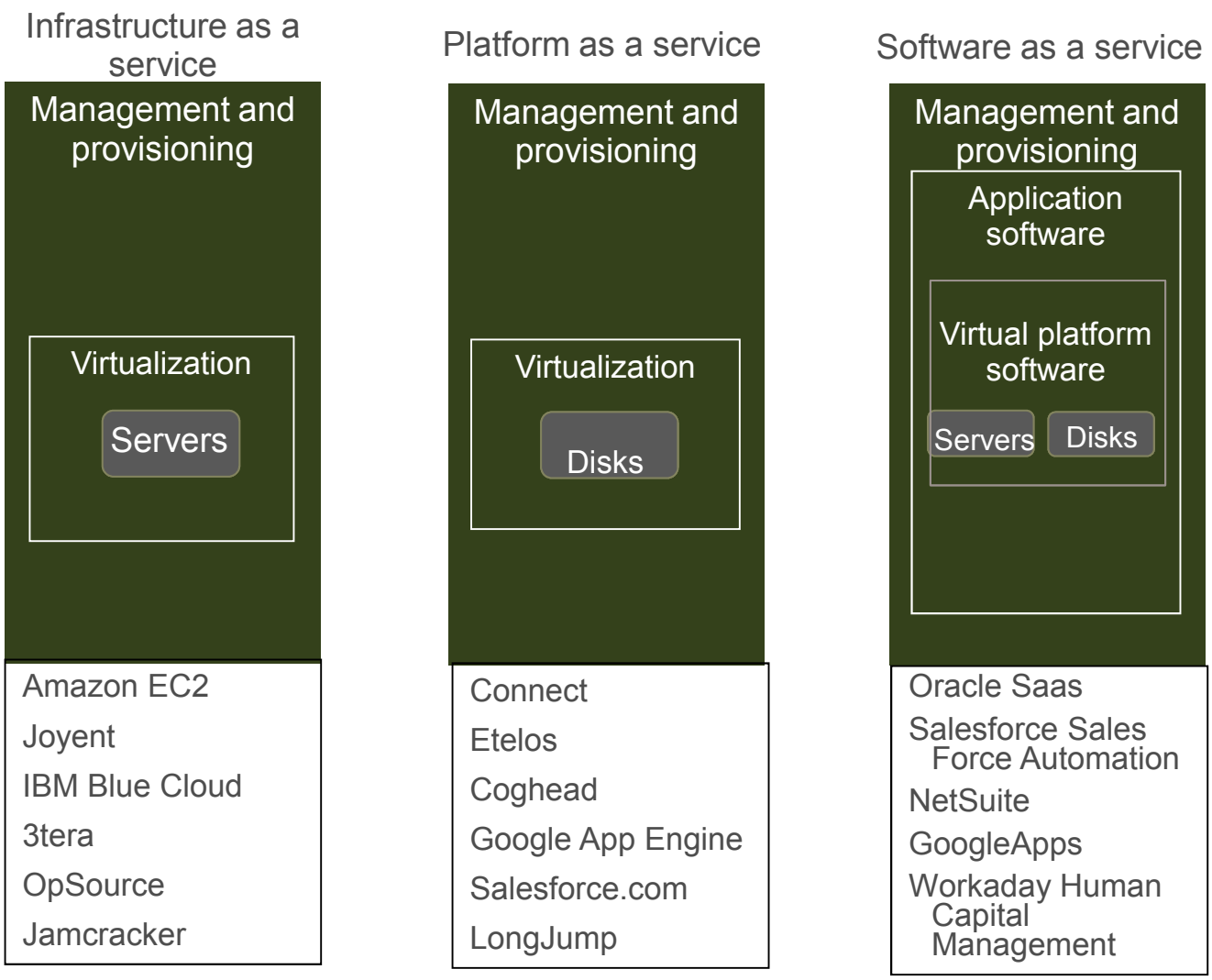
EMAGINED SECURITY

- There is no general agreement concerning exactly what the term “cloud computing” means
  - Wikipedia provides as good a definition as there is by defining cloud computing as “the provision of dynamically scalable and often virtualized resources as a service over the Internet on a utility basis. Users need not have knowledge of, expertise in, or control over the technology infrastructure in the ‘cloud’ that supports them.”
- Common characteristics of cloud computing include
  - Shared resources
  - Massive scalability
  - Elasticity
  - “Pay as you go”
  - Self-provisioning of resources



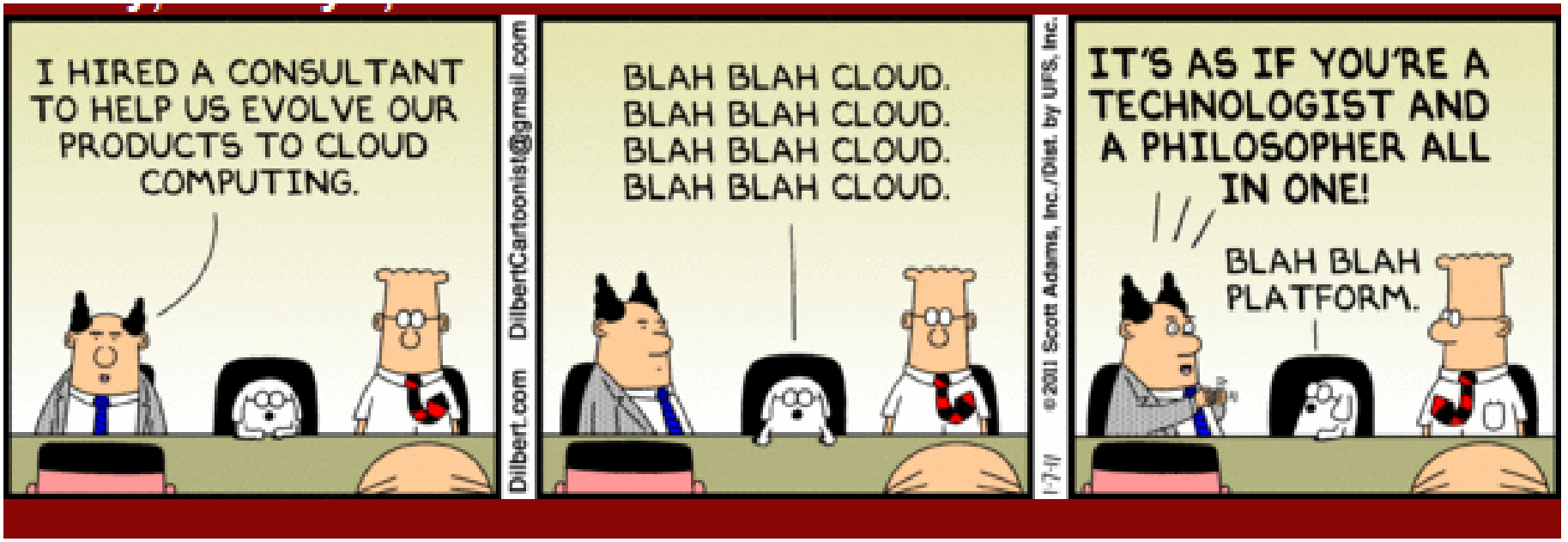
Major types of cloud computing

EMAGINED SECURITY



One of the major problems with cloud computing

EMAGINED SECURITY



Major cloud security risks (1)

EMAGINED SECURITY

- Higher data security risk
- Higher denial of service risk
- Elevated chance of break-ins and session hijacking
- Unavailability of custom security features
- Potentially greater insider risk
- Obstacles to
  - Incident response and forensics
  - Business continuity and disaster recovery
  - Auditing

Major cloud security risks (2)

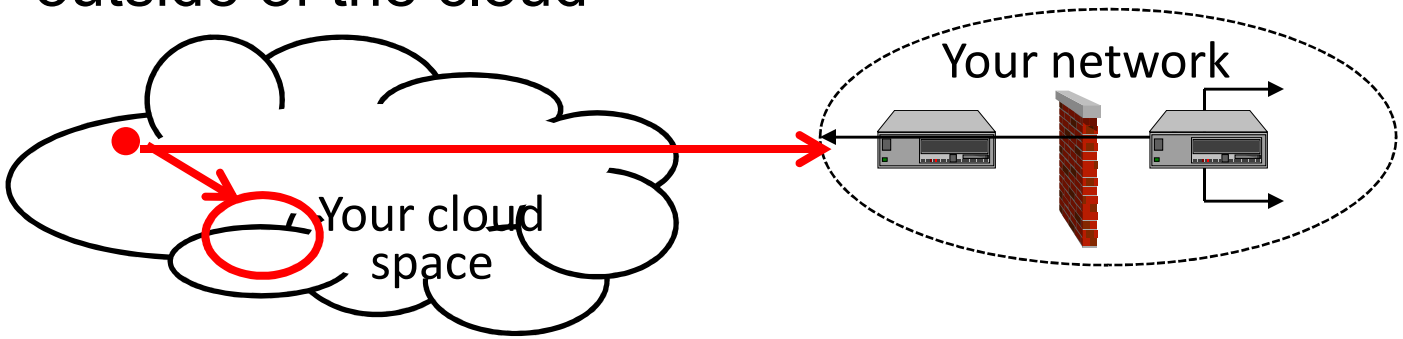
EMAGINED SECURITY

- Elevated legal and compliance risks
- Distributed security controls among different cloud service providers
- More…

Cheap accounts—often the starting point for big cloud attacks

EMAGINED SECURITY

- Problem--ease and immediacy of obtaining free or nearly free accounts
  - User identities are often not checked
  - Accounts are often poorly monitored (if at all)
  - Hackers may each amass hundreds of these accounts
- Accounts are used to
  - Launch attacks against computing systems within and outside of the cloud



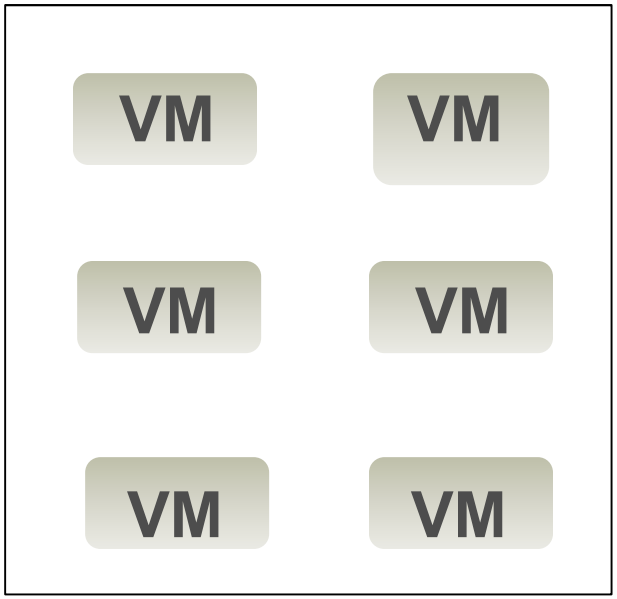
  - Build botnets that generate massive spam and cause massive distributed denial of service attacks

Cheap accounts—Amazon EC2

- Amazon EC2 “throwaway accounts” have been used to
  - Build massive botnets in which each bot has stolen passwords
  - Steal user credentials and use them to break into accounts
  - Attack sites all over the Internet (including Sony Entertainment servers recently)

Exploitation of vulnerabilities in virtualization software (1)

- Virtualization is used extensively in connection with IaaS (and also often with PaaS) cloud services
- Virtualized environments feature multiple Virtual Machines (VMs) within each physical host



Exploitation of vulnerabilities in virtualization software (2)

- Unauthorized superuser access to the host VM results in unauthorized superuser access to all guest VMs on the same physical machine
- “Hyperjacking” can result in unauthorized control of the entire virtualized environment within a physical machine
- VM escapes can allow users with access to a guest VM to gain access to other VMs (including the host VM) on the same physical machine
- A hostile VM may be able to access disk space used by other VMs

Exploitation of vulnerabilities in virtualization software (3)

- Man-in-the-middle attacks during VM migration can result in an attacker gaining full control of the migrated VM
- Network security barriers (e.g., firewalls) that work effectively in conventional network environments may work differently (or may not work at all) in virtualized environments

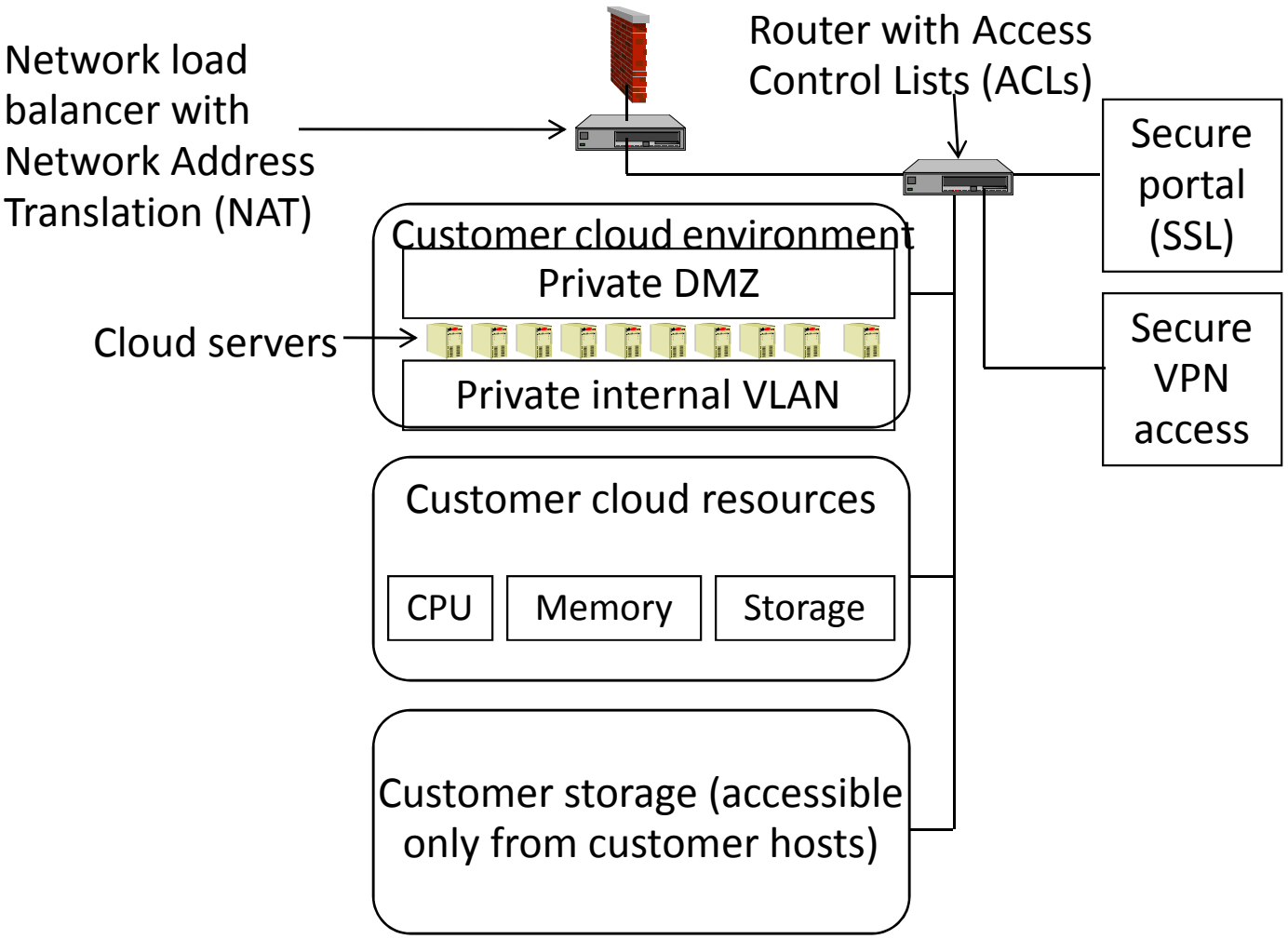
Denial of service in the cloud

- The interface between cloud services and conventional networks is the Internet
  - Internet is highly vulnerable to massive denial of service (DoS) attacks
- Cloud service providers face special issues concerning throttling incoming network traffic
  - Regulation of throughput rate could adversely affect customers
- Cloud networks are proving to be a safe haven for myriads of bots that could at any time be unleashed to launch massive DoS attacks

Exploitation of “cloudware”

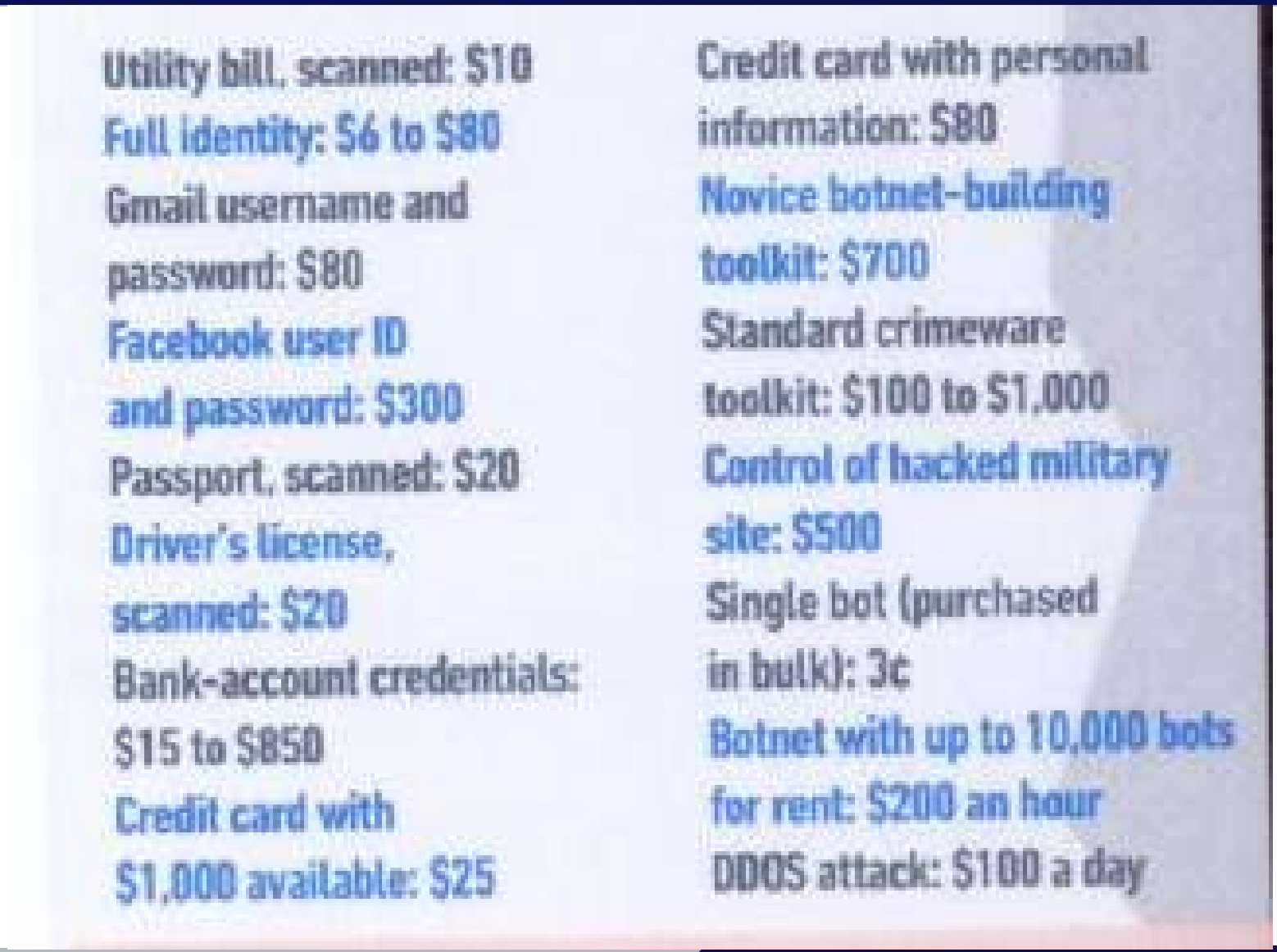
- Cloud service providers have rushed to develop and release “cloudware”
- Problems include
  - Haste in code development
  - Lack of sound software engineering methodology
  - Exclusion of security engineering (often, but not always)
  - An accumulating mass of cloud-related proprietary software
- The attacker community is spending a great deal of time and effort in discovering and exploiting cloudware vulnerabilities

Exploitation of cloud portals



The cloud: An enabler of all kinds of fraud and attacks

EMAGINED SECURITY



Encouraging developments in cloud security

- “Digital Ants” (Pacific Northwest National Laboratories)
- HyperSafe (North Carolina State University)
- New Chrome Notebook—all writes are in the cloud, not to the local computing system
- “Write-proof” hard drives

Conclusion

EMAGINED SECURITY

- Many cloud security risks are similar to risks in conventional computing and network environments, yet some are unique to cloud environments
- Many cloud risks are the result of cloud service providers trying to make things easier and cheaper for cloud customers
- “Hacking the cloud” can be incredibly easy
- “Rushing to the cloud” can prove to be one of the biggest mistakes your organization can make
- Several new research developments may potentially make a large difference in efforts to achieve suitable levels of cloud security

Questions?

EMAGINED SECURITY

Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
USA
+1 (650) 593-9829
eugeneschultz@emagined.com
Web: www.emagined.com
Blog: baylinks.com/blogs
Dashboard: dashboard.emagined.com

For a PDF copy of these slides send email to:
seminar@emagined.com