Spread Spectrum IP™
NextGen Performance and Cyber Protection In YOUR WORLD

UNPRECEDENTED SECURITY
EXTRAORDINARY RESILIENCE
INCREASED SPEED/PERFORMANCE
What does a utility of the 21st Century look like?
CHANGES ARE COMING

A Super Smart Grid

1. **Saving money**: Uses technology to help us optimize our homes and businesses so we can buy electricity at the cheapest rates.

2. **Making money**: A smart grid allows everyone to sell unused power back to the system. A smart grid meter spins both ways.
CHANGES ARE COMING

Elon Musk
- Founder and CEO of PayPal
- CEO Space X
- CEO Tesla Motors

SolarCity
Summary
This research introduces a series of documents intended to assist planning efforts for IT and OT integration in an uncertain future. CIOs and IT leaders should read this series to understand multiple, possibly disruptive futures for the intersection of IT and OT management.

The 'Uncertain Outcomes' Future of IT/OT Management
13 December 2013  G00259078
Analyst(s): Kristian Steenstrup / Geoff Johnson
Summary
The "uncertain outcomes" future has highly fractured and isolated IT/OT systems and processes, with OT management practices dominating in isolation from IT industry disciplines, despite strategic corporate focus by CIOs and IT leaders.
The 'Frustration Pit' Future of IT/OT Management
13 December 2013  G00258452

**Analyst(s):** Kristian Steenstrup | Geoff Johnson

**Summary**

The IT/OT "frustration pit" is characterized by an urgent and tactical interest in creating corporate agility around a highly fragmented enterprise's existing IT/OT management. This research helps CIOs and IT leaders understand this possibly disruptive future for the intersection of IT and OT.

The 'Agile Operations' Future of IT/OT Management
13 December 2013  G00259079

**Analyst(s):** Kristian Steenstrup | Geoff Johnson

**Summary**

This agile operations future presents a world where CIOs and IT leaders recognize the value of systematically applying IT management techniques to the governance and functioning of operational technologies, with a view to improving total corporate performance, business analysis and reporting.
The 'Optimized Operations' Future of IT/OT Management
13 December 2013  G00259080

**Analyst(s):** [Kristian Steenstrup](#) / [Geoff Johnson](#)

**Summary**
The optimized operations future presents a world where CIOs and IT leaders have recognized the strategic value of applying IT management techniques to the functioning of operational technologies, and have made optimal changes to improve total corporate performance.

The Utility in the 21st century will be a DATA DRIVEN organization
Cyber Attacks are Increasing

855 INCIDENCES, 174 MIL RECORDS COMPROMISED
2012 DATA BREACH INVESTIGATIONS REPORT

“Wide Cyber Attack Is Linked to China” Security researchers said they have discovered software capable of stealing information installed on computers in 103 countries from a network that targeted government agencies.

A Congressional survey of utility companies has revealed that the country's electric grid faces constant assault from hackers, with one power company reporting 10,000 attempted Cyber Attacks per month.

Citigroup: Hacker’s accessed over 360,000 credit card accounts and stole about 2.7 million dollars
CNN Money – June 2011

BlueCross BlueShield of Tennessee recently struck a deal to pay $1.5 million in penalties to the U.S. Department of Health and Human Services as a result of a data breach that violated the Health Insurance Portability and Accountability Act

Dispersive Proprietary
Cyber Attacks are Increasing
**DISPERSED PATENTS**

**Virtual Dispersive Routing**

**Private Peering of Virtual Networks**

**Multiplexed Client Server (MCS) Communications and Systems**

**First 12 US Patents granted!**
Unprecedented Security

Dispersing the data over multiple paths eliminates the Man-in-the-Middle threat. Hackers can only obtain small pieces of the original file on any given pathway, rendering any data obtained meaningless.

Network Resilience

Reliability and Resilience go hand in hand. When a connection is lost on any one of several open pathways, data packets are then rerouted to an already existing path, or an additional path is established—resulting in negligible network downtime.

Speed / Performance

VDN traffic is dispersed over multiple independent paths using unique methods, increasing available bandwidth and optimizing data flows on individual pathways. Hence, speed and performance are increased.
Current products are good, but inadequate to fully secure our information. Man-in-the-Middle attacks are currently not effectively addressed.
VPN (Virtual Private Network) is a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks.

VPN Issues:

- **VPNs do not remove all risk from networking.** Encrypted traffic can be intercepted as it is transmitted via a single path, and Encryption algorithms can be broken. *$20 decryption software is available on the Internet from Cloud Cracker*

- **Encryption key disclosure.** An attacker who possesses a key could not only decrypt traffic, but potentially also pose as a legitimate user.

- **Decreased Availability.** Many VPN implementations decrease availability because they add more components and services to the existing network infrastructure.
• VDN is also a virtual network built on top of existing physical networks that can provide a secure communications mechanism for data and control information transmitted between networks but was developed as a military grade solution to address the issues associated with VPN
  – **Better Security.** VDN provides multiple simultaneous paths for data transport to obfuscate data. Each path uses its own encryption and carries only a fraction of the data, greatly reducing the ability to intercept, decrypt and analyze the data. The path, encryption, port and IP addresses are continuously shifting greatly increasing the complexity and time required for an intruder to find and decrypt traffic
  – **Data Integrity and Identification Verification.** Only other trusted peer VDN communication is recognized preventing an intruder from posing as a legitimate user
  – **Increased Availability & Resiliency.** VDN greatly improves availability by providing authorized users access through any VDN enabled device. VDN utilizes existing networks reducing the hardware requirements of a VPN configured network
  – **Improved Performance.** Additionally VDN noticeably improves network performance (*measured 2 to 4½ times throughput improvement over VPN*) and VDN will reroute traffic with network degradation, improving resiliency
VDN Drivers are inserted between the Operating System and a Device’s Network Interfaces (at layer 2 in the network stack).

VDN Drivers enable Signaling, Routing and Control of Peer-to-Peer Network Communications between Devices Running VDN Software.
We put routing on all clients to force independent routes.

Routers Control Transmission on the Internet.

WHY IS VDN POSSIBLE?
100% Software Solution or Dedicated Gateway Hardware

 Installs on existing computers & devices

 Protects Integrity of Network
 If hacker penetrates a network device, he will not be able to move to, or affect other devices on network

 Denial-of-Service Attack (DDoS)
 Network continues to function

 With VDN, we can firewall everything in the “cloud.”
Dispersive Presence Server (DPS) acts as “address book” for network. No data passes through the DPS.
When the data passes through other devices, on their independent paths to the recipient, we call it a deflect.
Deflects do not store or decrypt any traffic.

When the data passes through other devices, on their independent paths to the recipient, we call it a deflect.
EXAMPLE: FORCES INDEPENDENT NETWORK PATHS

Multiple Simultaneous Network Paths for VDN Enabled Devices Provide Enhanced Security and Performance
Multiple Simultaneous Network Paths for VDN Enabled Devices

Provide Enhanced Security and Performance

Final packet received and message successfully re-assembled

EXAMPLE: FORCES INDEPENDENT NETWORK PATHS

Transmission Paths from Client One to Client Four
Path 1  
Path 2  
Path 3  

VDN Enabled Devices
Internet Routers

Client

Data Center

VDN Switch
Packet injection allows data to become compromised while being transmitted to its destination.

The message is compromised by a hacker who intercepts a portion of the data and sends the compromised packet along its route to the destination.
Multiple Simultaneous Network Paths for VDN Enabled Devices
Provide Enhanced Security and Performance
When a compromised packet is detected, a new packet is sent to allow the data to be re-assembled at the destination.
When the replacement packet is received, the message is re-assembled and the hacker’s attempt fails.
Dispersive networking detects hacking including nano-bots
Virtual Machine isolates attacker from application data
Prevents piracy/exfiltration due to authentication and trusted peer registration

DETECTION OF NETWORK ATTACKS

VDN Intrusion Response

1. Send Not-Us Traffic up to the OS
2. Drop Not-Us Traffic
3. Reroute Traffic to Analysis Server
   - Change IP address for Us Traffic
   - Shift Port for Us Traffic

Internal Threat Data Exfiltration

- Exfiltration Point would require VDN Software
- Exfiltration Point would have to be registered on the VDN Switch as a trusted peer
  - (Would require access to VDN Switch)
VERTICALLY LAYERED COMMUNICATION

Single Encryption Key at each path

Application
OS
VDR
Dispersive
Encryption
Hardware

VM – Virtual Machine
OS – Operating System
VDR – Virtual Dispersive Routing
NIC – Network Interface Card

Dispersive Proprietary
Multiple Simultaneous Network Paths
Different Port, Different Encryption for each Path
Provides Enhanced Security and Performance
Multiple Simultaneous Network Paths
Different Port, Different Encryption for each Path
Provides Enhanced Security and Performance
Multiple Simultaneous Network Paths
Different Port, Different Encryption for each Path
Provides Enhanced Security and Performance
Acronym List
VTC – Virtual Thin Client
ETH - Ethernet
SSP - Spread Spectrum Protocol
UDP - User Datagram Protocol
TCP - Transmission Control Protocol
DomU - Domain User

Layer 2 and 3 Interface

- **VTC\text{APPLICATION}**
  - Peer-To-Peer Setup
  - TCP-UDP Conversion
  - Encryption
  - SSP

- **VTC\text{KERNEL}**
  - Bridge (Layer 2): AES 256
  - Route In (Layer 3): AES 256
  - Route Out (Layer 3): AES 256

- **Domain**
  - DomU

- **NIC**
  - ETH 0
  - ETH 1
  - ETH 2
  - ETH 3

- **Control**
- **SSP Encryption**

Dispersive Proprietary
Two Implementations

- Single OS
- Fully Virtualized Environments
• **FIPS 140-2 Certification**
  – National Institute of Standards and Technology testing
  – Half complete
    • Notified on 10/29 that mobile testing was complete and certificate #2013 awarded

• **DHS Safety Act Designation**
  – Independent assessment of our product’s utility in protecting the nation’s energy grid from a terrorist attack
  – It provides protection from litigation if there is a perceived failure of our software that is being used to protect critical infrastructure systems

• **DISA Certification**
  – Certification effort underway
  – Beginning of the process to achieve ATO (expected by 5/2014)
  – Will provide access to NIPR SIPR networks

• **Air Force Networks Accreditation**
  – Certification effort underway using and AFRL to identify an appropriate network for evaluation that will lead to accreditation
Patented Network Operating System

Operates at the MAC and Link layer (below the O/S) offering improved security and efficiency over products operating at higher layers
  • Implementation does not require modification of proprietary applications
  • Improved QOS / ROS
    • Maintains service during an attack
    • Recognizes data stream failures and redirects connections

Software solution is less expensive and more versatile than a hardware solution

Multi-path routing to avoid interception / man-in-the-middle

Secure, non-traceable communication of sensitive information

Platform agnostic P2P communications between dissimilar devices and through firewalls

Reduced carrier backbone requirements / bandwidth

Watermarked packets ensure data integrity and identity verification

Single Key Encryption (flexible/low crypto overhead)

Dynamic and locally controlled White Listing

Enables Beaconing and mapping of network attacks through multiple means for forensic purposes
Michael D Seymour  
VP of Information Technology  
mseymour@pike.com  
(336) 719-4428

Rob “Moose” Smith  
VP of Business Development  
rsmith@dispersivetechnologies.com  
(702) 994-0687

www.dispersivetechnologies.com