Wireless Security Perspectives

Cellular Networking Perspectives

Technical Editor: Les Owens, Managing Editor: David Crowe Vol. 2, No. 10. November, 2000

CryptoNews: VPNs are taking off

Today, the Internet and the Web are ubiquitous. Companies are able to capitalize on the ubiquity of the Internet for business purposes through the use of "extranets" (see Figure 1), extending and connecting their internal networks ("intranets"). However, extending a company's network to the outside world across the Internet presents major network security concerns.

The Internet is subject to many threats:

- Data that is transmitted needs to be protected against malicious tampering and from prying eyes, provided with both integrity and confidentiality.
- Protection is also needed against identity spoofing and denial-of-service attacks.
- Access to a company's networks and its resources must be protected against unauthorized access.

Companies can extend their networks today through the use of a VPN (Virtual Private Network), which is simply a private network built on top of a public network. For a secure VPN, computer hosts within the private network should use cryptography to communicate securely. The cryptography, or encryption, excludes hosts from outside the private network even both utilize the public network for data transport (see Figure 2).

Many VPNs are designed around industry security standards – specifically, standards developed by the Internet Engineering Task Force (IETF). The IETF created the IPSec (Internet Protocol Security) suite as a basis for the security of VPNs. Yes, the Internet is everywhere and the economics of using this public network are compelling for companies. VPNs, therefore, are becoming a strategic necessity for most companies, hence their development and use is exploding. In the wireless environment, the need for cryptographic protection is perhaps even greater. Companies are looking at using VPN technology for securing the insecure radio environments.

IPSec is a standards-based method for providing privacy, integrity and authenticity to information transferred across IP networks. The goal of IPSec is to address all of the threats mentioned above in the network infrastructure itself. IPSec does this – without requiring expensive host and application modifications – by providing IP network-layer encryption.

IPSec standards define several packet formats: the authentication header (AH) to provide data integrity, and the encapsulating security payload (ESP) to provide confidentiality and data integrity. The redoubtable problems of Key Management and security associations (the IPSec parameters between two devices) are resolved through Internet Key Exchange. IKE can use public key certificates for device authentication to enable the creation of large, secure networks – digital certificates address key management issues and allow scalability.

For more information on these new cryptographic VPN devices, and for informa-

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security* Perspectives is $250 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$300 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

Current subscribers to Cellular Networking Perspectives receive a discounted price – only $200 for delivery within the US and Canada or $250 elsewhere.

Back issues are available individually, or in bulk at reduced prices.

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

December 15th, 2000.

Future Topics

IP security • Public Keys & Wireless • Kerberos PKINIT• Public Key Infrastructure (PKI) • IKE • Wireless Data Security • IETF Security Standards • AES (Rijndael)

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. Phone: 1-800-633-5514 (+1-403-274-4749) Fax: +1-403-289-6658 Email: cnpsales@cnp-wireless.com Web: http:/www.cnp-wireless.com/wsp.html. Subscriptions: $200 for current Cellular Networking Perspectives subscribers for delivery in the USA or Canada, US$250 elsewhere. Non-subscribers pay $250/yr. for delivery in the USA or Canada, US$300/yr. elsewhere. Payment is accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. Delivery: Email or 1st class mail. Back Issues: Available individually for $20 in the US and Canada and US$25 elsewhere, or in bulk at reduced rates. Discounts: Educational and small business discount: 25% off any order. Copies: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Figure 1: Internet Usage – Insecure

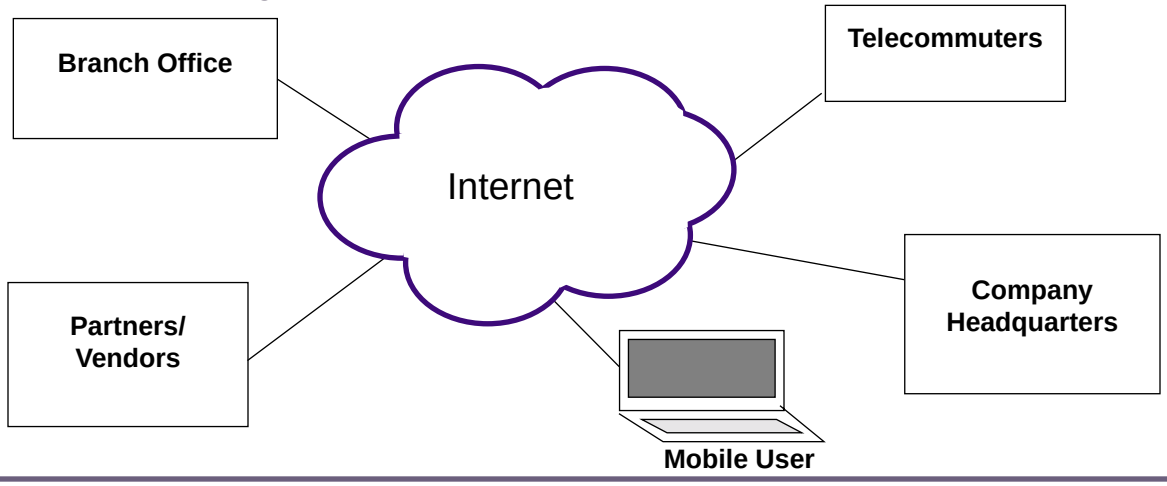
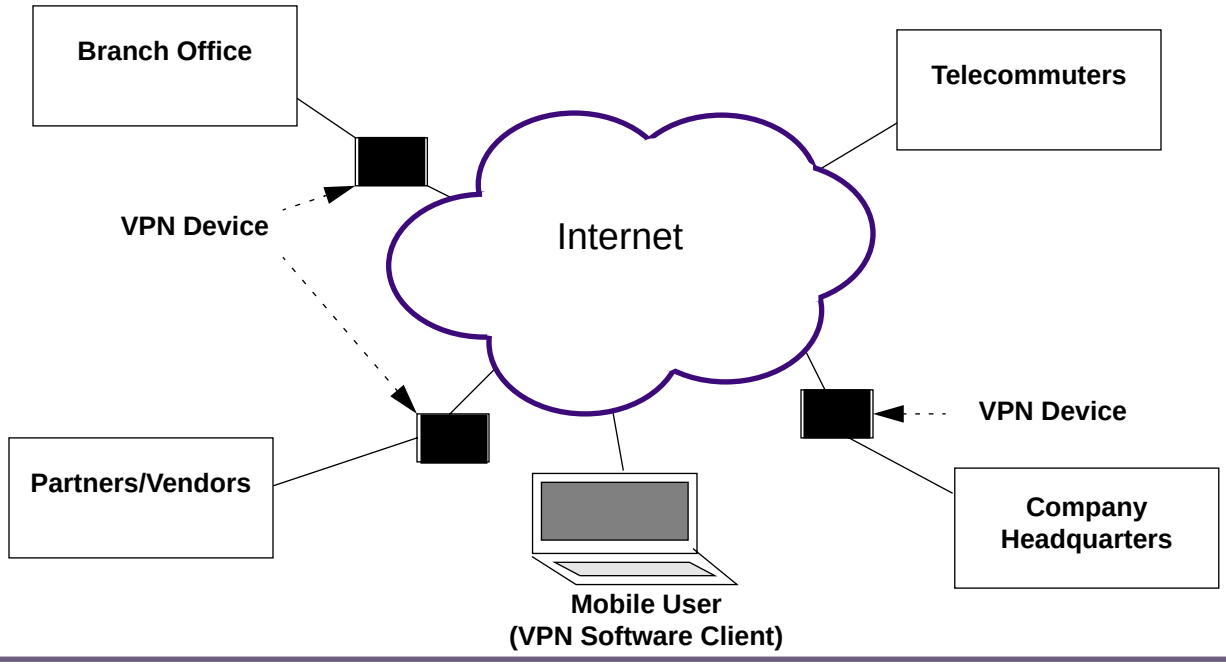


Figure 2: VPN Devices for Cryptographic Security



tion on the companies manufacturing them, visit:

www.vpnc.org

For information on Internet Engineering Task Force (IETF) and the IPSec protocol suite, visit:

www.ietf.org

IETF RFCs for IPSec

The twelve specific RFCs (Requests-for-Comments) comprising the IPSec protocol suite are the following:

1. Security Architecture for the Internet Protocol:
   www.ietf.org/rfc/rfc2401.txt?number=2401
2. IP Authentication Header:
   www.ietf.org/rfc/rfc2402.txt?number=2402
3. The Use of HMAC-MD-96 within ESP and AH:
   www.ietf.org/rfc/rfc2403.txt?number=2403
4. The Use of HMAC-SHA-1-96 within ESP and AH:
   http://www.ietf.org/rfc/rfc2404.txt?number=2404
5. The ESP DES-CBC Cipher Algorithm With Explicit IV:
   www.ietf.org/rfc/rfc2405.txt?number=2405
6. IP Encapsulating Security Payload (ESP):
   www.ietf.org/rfc/rfc2406.txt?number=2406
7. The Internet IP Security Domain of Interpretation for ISAKMP:
   www.ietf.org/rfc/rfc2407.txt?number=2407
8. The Internet Security Association and Key Management Protocol (ISAKMP):
   www.ietf.org/rfc/rfc2408.txt?number=2408
9. The Internet Key exchange (IKE):
   www.ietf.org/rfc/rfc2409.txt?number=2409

10. The NULL Encryption Algorithm and Its Use with IPSec:
    www.ietf.org/rfc/rfc2410.txt?number=2410
11. The IP Security Document Roadmap:
    www.ietf.org/rfc/rfc2411.txt?number=2411
12. The OAKLEY Key Determination Protocol:
    www.ietf.org/rfc/rfc2412.txt?number=2412

Upcoming Security Conferences – What's Happening?

ShadowCon Security Conference
28 November 2000
Naval Surface Warfare Center
Dahlgren, Virginia
www.technologyforums.com/0damain.htm

Cyber Sabotage Conference
29-30 November 2000
Hilton-Alexandria (Old Town)
Alexandria, VA
www.iqpc.com

E-Security Conference and Exposition
30 November-1 December 2000
Arlington, VA
www.intmedgrp.com/security

14th Systems Administration Conference
3-8 December 2000
New Orleans, LA
www.usenix.org/events/lisa2000

VPN 2000 – Implementation and Management
4-6 December 2000
Eden Roc Resort, Miami, Florida
www.icmny.com/SBRPages/VPN2K/vpn2kpro.htm

Capital SANS
10-15 December 2000
Capital Hyatt, Washington, DC
www.sans.org/capsans.htm

Internet Engineering Task Force
10-15 December 2000
San Diego, CA
www.ietf.org/meetings/IETF-49.html

Abelian Varieties – Optimal Cryptography for Wireless Communications?

V. Kumar Murty

This month's issue of *Wireless Security Perspectives* is the third in a 3-Part series on Public Key Cryptosystems (PKCS) for wireless communications. The first part, co-authored by Certicom, described why Elliptic Curve Cryptography (ECC) is being considered by the wireless industry for the cryptographic protection of communications. Last month, Boston-based NTRU Cryptosystems introduced another technique being considered for wireless industry security needs. In this issue, we conclude the series with a discussion by Toronto-based Karthika Technologies on a very advanced number-theoretic form of PKCS – *Abelian Varieties*.

With the rapid development of CDMA and other second-generation cellular technology, wireless communications have experienced an unprecedented period of growth. In 2000, there are an estimated 600 million wireless subscribers worldwide. By all indications, this growth is far from peaking, and we are just at the beginning of a long upward climb. In fact, the number of wireless subscribers should exceed 1.2 billion in 2003. However, this phenomenal burgeoning of the field has also led to new security concerns.

One of the reasons that wireless devices are vulnerable to additional security risks is that they are computationally constrained environments. This means the all-important cryptographic key-size, one of the key variables (no pun intended) used to measure the security of the system, has to be kept small. Manipulating larger key sizes during cryptographic processing simply overpowers or significantly slows down the system's processor. The same considerations we are about to discuss apply to PDA's, wireless tablets and any small hand-held wireless computing device.

In the wireless domain, therefore, significant research is ongoing for cryptographic protocols that offer high levels of security with relatively small key sizes. It is here that AVC – Abelian Variety Cryptosystems – offer a potential solution. A cryptographic scheme using a two-dimensional Abelian variety over a finite field of size approximately 2^{87} can give security comparable to that achieved with an RSA system over a field of size approximately 2^{1024} or an ECC system over a field of approximate size 2^{173}. This potential for significantly reducing the field size without compromising security is why AVC is seen by some as the optimal cryptographic scheme for wireless communication security.

Public Key Cryptography

Many public key cryptographic protocols are based on an algebraic object called an Abelian group G[1]. An Abelian group is a set in which we have one arithmetic operation that we denote *. Thus, given two elements (g and h) in G, the operation g*h produces another element in G. This operation is commutative in the sense that g*h = h*g. Given a number x, we write g^x to denote g * ... * g (x times). Thus, $g^1 = g$, $g^2 = g*g$, $g^3 = g*g*g$, etc. The group must satisfy other familiar mathematical properties (axioms) which we will not review here.

In general, if we are given g and h, and if we are told $h = g^x$ for some value of x, it is a difficult problem to find x. This is called the discrete logarithm problem (DLP) as we discussed briefly in the September issue of *Wireless Security Perspectives.* The difficulty of this problem is what is exploited for cryptography.

Suppose that user A (Alice) and user B (Bob) want to communicate over an open channel using the group G. The basic El-Gamal encryption method proceeds as follows:

1. Each selects a secret key – x for Alice and y for Bob.
2. Each computes and publishes (perhaps with a certificate authority) the

1. Abelian groups are named after Niels Henrik Abel (1802-1829), the Norwegian mathematician first to study them.

public key, g^x for Alice and g^y for Bob.

Now, if Alice wants to send a secure message to Bob, she:

1. Converts the message to an element (or a sequence of elements) in G – call it m.
2. Selects a random integer k
3. Transmits the pair, (g^k, mg^{ky}).

When Bob receives this, he uses his secret key (y) and applies it to the first element to compute:

$(g^k)^y = g^{ky}$

He then uses this to unmask m:

m = (the second component)*g^{-xy}

Note that it would have been extremely difficult for anyone except Bob to perform this operation because they would not know y and without y, it is difficult to compute g^{xy}. This is the difficulty of the discrete logarithm problem in the group G.

The Choice of Group

Each of many possible Abelian groups offers a cryptographic protocol. What makes one more desirable than another? There are two considerations:

- The ease with which one can compute in the group; and
- The difficulty of solving the discrete logarithm problem.

Currently in use are the multiplicative group of nonzero elements in a finite field and the group of points on an elliptic curve over a finite field. Karthika Technologies is developing a third: the group of points on an Abelian variety over a finite field. In all of these cases, one has to exercise some care in the choice of finite field, elliptic curve and Abelian variety to see that the two considerations mentioned above are satisfied, in particular, the second one.

What is an Abelian variety?

Abelian varieties are higher dimensional versions of elliptic curves. The extra degree of freedom given by the dimension is what allows for the decrease in field size without reducing security.

An elliptic curve can be described by a single equation. Usually, it can be written in the form

$y^2 = x^3 + ax + b$

for some coefficients, a and b. The space of elliptic curves forms a one-dimensional family.

By contrast, Abelian varieties require many equations. For example, over the complex numbers, a two-dimensional Abelian variety can be described by 13 quadratic equations. Moreover, these equations are not easy to describe explicitly. But this difficulty in describing Abelian varieties is compensated for by their abundance. While elliptic curves form a one-dimensional family, over the complex numbers, two-dimensional Abelian varieties form a three-dimensional family. Three dimensional Abelian varieties form a family of six dimensions, four dimensional Abelian varieties live in families of ten dimensions, and so on. Even over finite fields, the size of the family of Abelian varieties grows with the dimension. Thus, once the problem of describing them in some efficient form is solved, we have many more choices for the basis of a cryptographic protocol.

At the same time the equations are made precise, we also make explicit the group law on the variety. The group law refers to the way in which two points on the geometric object are combined to form a third point on the same object. Recall that the message to be communicated is first converted to a series of points on the Abelian variety. It is then encrypted using the recipient's public key by using the arithmetic – that is, the composition law – on the Abelian variety.

Jacobians of curves

In some cases, the time required for these calculations can be reduced significantly. This can be done when one deals with Jacobians of curves. The Jacobian construction is a classical method for producing a higher dimensional Abelian variety from a one-dimensional curve. This curve is not an elliptic curve in general, and the curve itself does not have a composition law. Thus the curve cannot be used for cryptography. However, through the Jacobian construction, one produces a larger object – namely, an Abelian variety – on which there is a composition law.

Jacobians have been studied extensively for applications in cryptography. One case which has received more attention than others, beginning with the work of Koblitz and Cantor, is that of the Jacobians of hyperelliptic curves. Such curves are in general given by an equation of the form

$y^2 = f(x)$

where f is a polynomial of some degree d. For example,

$y^2 = x^5 + x^4 + 3x^3 + 2x^2 + 1$

is a hyperelliptic curve with f of degree 5. Its Jacobian is an Abelian variety of dimension 2.

At present, the arithmetic on the Jacobian of a hyperelliptic curve is slightly slower than arithmetic on an elliptic curve over the same field. However, we gain a new advantage here over elliptic curves, and this is the entire motivation for studying them.

The Discrete Logarithm Problem (DLP)

The number of points on an Abelian variety A over a finite field of q elements is of the order q^d where d is the dimension. Thus, the above Jacobian has roughly q^2 points. An elliptic curve over the same field cannot have more than $q + 1 + 2q^{1/2}$ points. Thus an elliptic curve has a far smaller point set. Why do we care that the set of points on an Abelian variety is larger? The answer: Because it means the discrete logarithm problem – the acid test for security – is that much more difficult. Provided we have chosen our Abelian variety with care, the time to crack the DLP on a two dimensional Abelian variety is comparable to q units of time, while on an elliptic curve, it is $q^{1/2}$ units of time. Of course, the same proviso applies to the elliptic curve – it too must be chosen with care. Examples are specified in various draft standards such as the IEEE P1363.

Smaller Field Size for the Same Security

As an example, suppose we choose our curves over a field of $q \approx 10^{30}$ elements. This corresponds to approximately 90 bits, which is not a very large number in terms of the computing power available today. By using a straightforward baby step – giant step attack, the DLP on an elliptic curve over this field can be broken by checking about 2^{45} keys. The same attack on this Abelian variety would require checking about 2^{90} keys, a number close to the age of the universe. This gives an idea of the quantum leap in security one stands to gain by developing AVC. In this context, it should be noted that ECC, over a field of size 108 bits, is now considered weak.

In a finite field protocol, a field of size N (and so about log N bits) offers approximately

$$\exp\left(c(\log N)^{1/3}(\log \log N)^{2/3}\right)$$

amount of security. (Here, c is a positive constant which can be made explicit.) On the other hand, ECC offers security of the level

$$N^{1/2}$$

In contrast, an Abelian variety of dimension d should offer security of level

$$N^{d/2}$$

The Road Ahead

Before AVC can become a commercial reality, much technical and mathematical work remains to be done. At present, there are two major drawbacks. First, the most obvious presentations of Abelian varieties require too many variables. Even in the case of the Jacobian of hyperelliptic curves, this means the key size is not reduced even though we are working over a smaller field. Second, computation in an Abelian variety of higher dimension tends to be slow. Over the past few years, much progress has been made in addressing these issues. Finding efficient presentations, together with speeding up and refining the method of calculation, constitutes the main focus for the research group centered at the University of Toronto and for its industrial partner, Karthika Technologies.

Glossary of Terms

Abelian variety. A geometric object with a group structure. Technically the object is "projective" and the group structure is "algebraic".

Curve. A one-dimensional geometric object. Usually, it can be specified as the set of points satisfying a single equation in two variables.

DLP. The discrete logarithm problem, is the difficult problem which ensures the security of the encryption.

Jacobian variety. A method of manufacturing an Abelian variety out of a curve.

Selected References

[1]. Blake, I., Seroussi, G., and Smart, N., *Elliptic curves in cryptography*, London Math. Soc. Lecture Notes 265, Cambridge Univ. Press, Cambridge, 1999.

[2]. Cantor, D. G., *Computing in the Jacobian of a hyperelliptic curve*, Math. Comp., 48(1987), 95-101.

[3]. Koblitz, N., *Hyperelliptic cryptosystems*, J. of Cryptology, 1(1989), 139-150.

[4]. Murty, V. K., *Introduction to Abelian varieties*, CRM Monograph Series, Amer. Math. Soc., Providence, 1993.

About the Author

V. Kumar Murty received his Ph. D. in Mathematics in 1982 from Harvard University. He is now professor of mathematics at the University of Toronto. He is also a Fellow of the Royal Society of Canada and a Steacie Fellow. He works on number theory, especially arithmetic aspects of algebraic geometry and automorphic forms. More recently, he has been focusing his attention on the cryptographic applications of Abelian varieties.

To Probe Further

For more information on Abelian varieties and the commercialization of the technology, contact either Kumar Murty at:

murty@math.toronto.edu

or Tony Chun at:

tchun@karthika.com

White papers and other information will soon be available at:

www.karthika.com

For more information on the IEEE's P1363 cryptographic standardization efforts, visit:

grouper.ieee.org/groups/1363/index.html